UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"ESTUDIO DE LA MIGRACION DE UNA RED LAN OPERANDO CON IPv4, A IPv6"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A:

MARCO ANTONIO CORDOVA MARTINEZ

DIRECTOR DE TESIS:
ING. JOSE LUIS PEREZ BAEZ

MÉXICO **2005**

CAPITULADO

3. PROTOCOLOS DE INTERNET

INTRODUCCIÓN

Situación actual.

El uso de Internet ha aumentado a tal grado que ya es común hablar de Internet en el hogar, empresas, oficinas, negocios, escuelas, celulares, aeropuertos, etc.
Este incremento en el uso de Internet ha provocado también el aumento del numero de aplicaciones desarrolladas para Internet de manera que es difícil enumerar la gran cantidad de aplicaciones para Internet.
Internet hoy en día se usa para todo y en todas partes, por lo que su uso se ha convertido en una necesidad para el desempeño de nuestras actividades diarias.
El protocolo de comunicaciones sobre el que basa su funcionamiento la Internet es el Protocolo de Internet IP, por lo que IP es el protocolo mas usado en el mundo ya que el crecimiento de la red Internet ha provocado a su vez un aumento cada vez mayor del uso del protocolo IP en las comunicaciones del mundo actual y sus perspectivas hacia el futuro es que su uso se extenderá todavía mucho mas.
El protocolo de IP en su versión 4 se ha convertido en el protocolo casi universal en las redes LAN, son pocas las redes que usan algún otro protocolo como IPX. A nivel WAN su uso también se ha extendido bastante, incluso hasta se ve ya como un protocolo que tiende a desplazar a otros protocolos como Frame Relay por ejemplo, puesto que la tendencia es llegar a tener redes IP únicamente que puedan manejar o hacer converger por la misma Internet voz, datos y video.
El protocolo IP además de ser usado para la comunicación en Internet, es usado en redes LAN, en redes inalámbricas, también se usa para el funcionamiento de un sinnúmero de aplicaciones como voz sobre IP, telefonía sobre IP, su uso se tiene proyectado para aplicaciones de telefonía celular donde se piensa implementar para proporcionar servicios como Internet móvil, se piensa usar en proyectos de interconectividad con dispositivos caseros como por ejemplo para que los refrigeradores se comuniquen por Internet para informar que necesitan ser aprovisionados.
Es tan variado y enorme el uso de IP así como las aplicaciones y proyectos que se tienen planeados desarrollar con este protocolo que un gran numero de esos proyectos y aplicaciones están detenidos o no se pueden desarrollar debido a algunos problemas que empieza a presentar este protocolo.
El mismo incremento en su uso y en las aplicaciones que funcionan sobre Internet han provocado que las características actuales del protocolo IPv4 presenten limitaciones que pueden convertirse en problemas serios en un futuro. Estas limitaciones o deficiencias a grandes rasgos son:

- El agotamiento del espacio de direcciones en poco tiempo.
- Deficiencias en la administración y distribución de las direcciones IP.
- Crecimiento de las tablas de ruteo en los ruteadores del núcleo de Internet, lo que puede llegar a causar problemas en el funcionamiento o desempeño de estos.
- En IPv4 no existen mecanismos que garanticen una buena calidad de servicio para tráfico crítico o especial como multimedia o video en tiempo real.
- IPv4 no posee características propias que proporcionen seguridad de los datos transportados por IP, la seguridad se tiene que implementar en capas superiores y con dispositivos adicionales lo que hace más complejo el funcionamiento de la red.
- La implementación de algunas de las medidas para resolver las deficiencias de IPv4 a su vez ha provocado otros problemas como la perdida del esquema de la

comunicación extremo a extremo, lo que dificulta aun más la seguridad de los datos, la comunicación de extremo a extremo, etc.
- Las limitaciones propias del protocolo IPv4 están impidiendo el despliegue total de muchos proyectos ambiciosos de aplicaciones sobre Internet.

Estas deficiencias sumadas a que el protocolo IPv4 desde su creación hace aproximadamente 40 años no ha cambiado y cuando se creo se creyó que los 4 mil millones (2^{32}=4 294 967 296) de hosts que podía direccionar serian suficientes, esta cantidad de direcciones para su época era bastante buena, el problema fue que nunca se vislumbraron detalles como el auge tan grande de Internet, una cifra de habitantes en el mundo mucho mayor que la de direcciones disponibles (hoy somos aproximadamente 6 mil 500 millones de habitantes) y que surgieran tantas aplicaciones que un momento dado se pudiera llegar a requerir mas de una dirección por habitante del planeta, por lo que en nuestros el numero de direcciones disponibles es un obstáculo para el desarrollo de nuevos proyectos de comunicación.

Para tratar de resolver las deficiencias de IPv4 se ha diseñado e implementado algunas medidas como:

- Reutilización de direcciones no utilizadas en una forma más eficiente.
- Utilización del ruteo interdominio sin clase CIDR (Classless Interdomain Routing) que elimina parcialmente el concepto de clases al representarlas por un prefijo y su longitud del prefijo con lo cual se reduce el desperdicio de direcciones y permite la agregación de las tablas de ruteo.
- Uso de direcciones privadas en forma interna a una red combinadas con el empleo de la traducción de direcciones NAT (Network Address Translation) para convertir esas direcciones a una(s) dirección(es) publica(s) para tener conectividad a Internet. Esta medida aunque tiene algunas ventajas también tiene muchas desventajas que se reflejan principalmente en obstáculos para el desarrollo de nuevas aplicaciones o implementaciones en Internet.

Estas medidas que realmente son un arreglo temporal de los problemas que esta enfrentando actualmente IPv4 han funcionado correctamente pero aun con estas medidas los problemas de IPv4 sumados a los que introducen estas medidas también a mediano o largo plazo se agravaran. Debido a esto desde el año 1992 se empezó a desarrollar una nueva versión del protocolo de Internet y para el año 1995 aproximadamente se propuso una definición del nuevo protocolo de Internet conocida como IPv6.

IPv6 fue diseñado para resolver los problemas y limitantes de IPv4 además de agregar nuevas características que lo hacen mas atractivo, dichas características tratan de cubrir las necesidades creadas por los grandes proyectos que se tienen actualmente para Internet.

El desarrollo tan enorme de la tecnología con el protocolo IPv4 y las técnicas implementadas para contrarrestar sus limitaciones tal vez han provocado que la adopción de IPv6 se retrase, pero en un futuro deberá llevarse a cabo para poder aprovechar las nuevas capacidades de esta versión en beneficio mundial. La transición a IPv6 necesitara ser alentada por medio de trabajos de investigación y pruebas sobre su funcionamiento en ambientes reales de producción.

Justificación

Actualmente son pocos los trabajos dedicados a explicar o estudiar el nuevo protocolo de Internet IPv6, las ventajas y desventajas de esta migración tecnológica y los beneficios sociales que trae consigo, ya básicamente solo las principales instituciones de educación superior del país han establecido proyectos para estudiar y probar este protocolo.
La importancia cada vez mayor del uso de Internet y su protocolo base IP genero la motivación para desarrollar un trabajo que ayude a conocer el nuevo protocolo IPv6 y que a la vez colabore en su divulgación.

Objetivo

El objetivo general de este trabajo es proponer un método de estudio y análisis de la migración tecnológica de una red LAN operando con IPv4 a IPv6, considerando todos los elementos implicados en el estudio.
Desarrollar un marco teórico del protocolo de Internet IPv6 que nos ayude a conocer sus características y funcionamiento.
Conocer como ayudaran las nuevas características de IPv6 a tener un mejor desempeño de las redes

Hipótesis

La nueva versión de Internet IPv6 permitirá a las redes LAN funcionar por lo menos al doble de su desempeño comparado con las redes que operan con Internet versión 4. El protocolo de Internet versión 6 permite minimamente duplicar la seguridad de la información.

Organización del capitulado.

En el capitulo 1, "Consideraciones Teóricas" se presentan algunos temas básicos de comunicaciones, este tema se implemento pensando en que todo desarrollo sobre comunicaciones debe tener siempre las bases o fundamentos ingenieriles que hicieron posible el desarrollo las comunicaciones.

El capitulo 2, "Modelo de referencia OSI y tipos de redes" trata el tema de las redes de datos, en este tema hablaremos de lo que son las redes, topologías, tecnologías, el modelo OSI, los componentes de interconectividad en redes, estos temas son la base de las redes LAN en la que se desea aplicar el uso de IPv6.

En el capitulo 3, "Protocolos" se habla del conjunto de protocolos TCP/IP, este conjunto de protocolos incluye dos muy conocidos que son TCP e IP, de los cuales IP es el objeto de este estudio, se estudian las diferentes versiones de IP (IPv4 e IPv6), sus datagramas, sus servicios, sus aplicaciones, en general se manejan las bases teóricas que permiten comprender el funcionamiento de IPv4 e IPv6, así como las características que diferencian a uno del otro y los mecanismos existentes para implementar la migración de IPv4 a IPv6.

Para el capitulo 4, "Red LAN propuesta para la migración tecnológica a IPv6" se presenta un panorama general del funcionamiento actual con IPv4, la topología y características de la red LAN en la que se desea aplicar la actualización.
En este mismo capitulo se realiza una propuesta de la red LAN con IPv6 presentando una serie de pasos a seguir para realizar la migración tecnológica donde señalaremos los cambios necesarios a realizar en los equipos y la red en conjunto.

El capitulo 5, "Comparativo de la migración" es usado para analizar el funcionamiento de IPv6 comparándolo con IPv4 para hacer notar sus características, y mejoras.

En el capitulo 6, "Evaluación y una recomendación técnica y económica" se hace un análisis económico para proponer un costo aproximado de la implementación de IPv6 en la red LAN.

Finalizamos con el capitulo 7, donde se presentan las "Conclusiones" obtenidas de este trabajo y de las pruebas realizadas.

1 CONSIDERACIONES TEORICAS

1.1 Sistemas de comunicaciones

En el contexto de la información y de las telecomunicaciones los sistemas son de gran importancia, a continuación mencionamos brevemente lo que es un sistema comunicación y sus partes que lo forman.

Concepto de Sistema

Un sistema es el conjunto de componentes o dispositivos del mundo físico que interactúan entre sí, que aceptan señales a su entrada, las transforman y generan otras señales a su salida. Es como una caja negra que transforma la señal a su entrada para generar la señal a su salida como muestra la Fig. 1.1.1

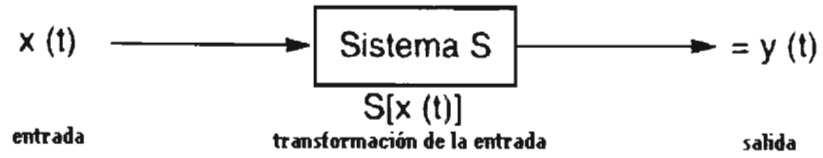


Fig. 1.1.1 Concepto de Sistema

Concepto de comunicación

Desde el punto de vista etimológico, la palabra "comunicación" proviene de la raíz latina *communicare*, es decir, "hacer común" algo.

Shanon en su obra Teoría Matemática de las comunicaciones describe a la comunicación como aquellos procedimientos por medio de los cuales una mente afecta a otra. Esto incluye voz, texto impreso o escrito, música, arte, teatro y danza. El mismo describe la comunicación entre maquinas como aquellos procedimientos por medio de los cuales un mecanismo afecta la operación de otro como por ejemplo el control de aviones.

La comunicación es el proceso mediante el cual se transporta información usando un código común entre un emisor o fuente y un receptor o destino. En nuestros días la comunicación se percibe más desde el punto de vista de la comunicación de datos en la cual se comunica información en forma binaria entre dos o más puntos.

Las comunicaciones siempre han sido importantes en la historia de la humanidad, pero han cobrado mayor importancia con el desarrollo de la tecnología y por la influencia que tienen en el grado de desarrollo de la sociedad, tal importancia se ha incrementado a tal punto que actualmente existen muchas variantes cada una con un significado y aplicación a determinado campo de actividad.

- Así tenemos las telecomunicaciones, el termino telecomunicación significa comunicar a distancia la mayor cantidad de información en el menor tiempo posible de una manera segura a través de un medio o canal de comunicación por medio de señales, esto se lleva a cabo con el uso de varias técnicas como modulación, codificación, compresión, formateo, multicanalización, esparcimiento del espectro, etc. Este es el término con el que se identifica actualmente más a las comunicaciones y cubre todas las formas de comunicación a distancia radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores.
- Informática que proviene de las palabras información, auto y matica que supone el procesamiento automático de la información.
- Telemática que es la conjunción de telecomunicaciones e informática e implica la transmisión y el procesamiento automático de la información.

Sucesos históricos que dieron origen a las telecomunicaciones.

Brevemente mencionamos a continuación algunos sucesos relevantes que dieron origen a las telecomunicaciones:

Se puede decir que las telecomunicaciones comenzaron con la invención del telégrafo que permitía tener comunicación usando el código Morse.

Posteriormente con el teléfono de Graham Bell empezó la comunicación de voz a distancia.

Después la aparición del teletipo o teleimpresor permitió enviar mensajes a distancia con el código Baudot.

Con la aparición del modem se implanto la conexión a distancia de computadoras y periféricos.

Mas tarde las telecomunicaciones y la informática se unen gracias a los lenguajes de programación interactivos y los sistemas operativos conversacionales junto con las tecnologías de conmutación de paquetes y satélites de comunicaciones.

Ya en los setentas hay una gran evolución de la conectividad apareciendo las redes de computadoras, protocolos y arquitecturas teleinformáticas.

Entonces se crea la red ARPANET que dio origen a Internet, desarrollándose junto con ella el conjunto de protocolos TCP/IP que ha influido tanto en las redes teleinformáticas.

En esta misma década se da el auge de la normalización, destacando la normalización de las redes de conmutación de circuitos y las redes de conmutación de paquetes. También se crea el modelo básico de referencia para la Interconexión de Sistemas Abiertos OSI.

A finales de los 70 aparecen las redes de área local que interconectan computadoras en un entorno reducido.

En los 80 se popularizan las Computadoras Personales y aparecen las redes digitales para integrar texto, datos, imagen y voz.

Actualmente en las telecomunicaciones se tiende al abaratamiento de la utilización de las redes así como nuevas posibilidades de transmisión proporcionadas por redes digitales de servicios integrados de banda ancha que operan a gran velocidad.

¿Qué es la Información?

Información tiene su origen en las palabras in y formare, que significa instruir hacia adentro.

La información es un fenómeno que proporciona significado o sentido a las cosas e indica mediante códigos y conjuntos de datos los modelos del pensamiento humano. La información procesa y genera el conocimiento humano. Los seres humanos han generado y perfeccionado tanto códigos como símbolos dándoles un significado y formando con ellos lenguajes comunes útiles para la convivencia a partir del establecimiento de señales y lenguajes para la comunicación.

La información es coleccionable, almacenable o reproducible. Se usa para tomar decisiones, conduce a obtener conclusiones acertadas o equivocadas, dependiendo de la información que se posea y como sea interpretada, así como de factores subjetivos y del contexto en que se encuentre la persona que la recibe o interpreta. La información no solo comunica noticias sino también estados de ánimo, opiniones o conocimientos

La función de la información es:

- Aumentar el conocimiento del usuario
- Proporcionar a quien toma la decisión, probabilidades para la elección, reduciendo la gama de decisiones
- Proporcionar reglas de evaluación y decisión para fines de control

Por estas y otras funciones a lo largo de la historia la información ha adquirido un gran valor. Actualmente nuestra sociedad es conocida como la sociedad de la información por la importancia que tiene el poseer, transmitir y administrar información, así como el tener la facilidad de procesar y transmitir esa información en modernos sistemas ya que esto lleva a tener un alto grado de desarrollo y por consiguiente gran influencia en el resto de la humanidad. La importancia de la información radica en que esta sea obtenida lo mas pronto posible y que sea desconocida ya que si a alguien le interesa cierta información ese interés decrecerá conforme el tiempo transcurra, o si el contenido es conocido esa información será irrelevante.

Desde el punto de vista de las comunicaciones, información es un patrón físico al cual se le ha asignado un significado comúnmente acordado, este debe ser único capaz de ser enviado por el transmisor y capaz de ser detectado y entendido por el receptor

La información puede ser medida, esta no se mide sobre la base de su longitud sino sobre la base de la probabilidad, ya que cuanto más probable es un mensaje menos información contiene.

La entropía es una magnitud que calcula la cantidad de información en un flujo de datos es decir lo que nos aporta sobre un dato o hecho concreto y se define como el valor medio de la información por símbolo:

$$H = \sum_{i=1}^{n} P_{x_i} I_{x_i}$$

las unidades son bits/mensaje.

Donde el contenido de la información de cada uno de los símbolos se define como:

$$I_x = \log_2 \frac{1}{P_x}$$

O en función de la probabilidad.

H = p1*log(1/p1)+p2*log(1/p2)+ .. pm*log(1/pm)

Donde:

- H es la entropía.
- p son las probabilidades de que aparezcan los diferentes códigos.
- m es él numero total de códigos.

Se utiliza el logaritmo en base 2 y la entropía se mide en bits.

La medición de la información o entropía se aplica a cualquier tipo de información y permite codificar esta información adecuadamente indicándonos los elementos de código necesarios para transmitirla, eliminando la redundancia. Nos indica el límite teórico para la compresión de datos.

¿Qué son los Datos?

Los datos constituyen a la información y son obtenidos con nuestros sentidos y a partir de ellos se genera la información para tomar decisiones. Los datos se han podido simbolizar en forma representativa.

Un dato es la cantidad mínima de información no elaborada y sin sentido por sí misma. Esta cantidad de información una vez obtenida y procesada forma lo que conocemos como información, como se muestra en la Fig. 1.1.2.

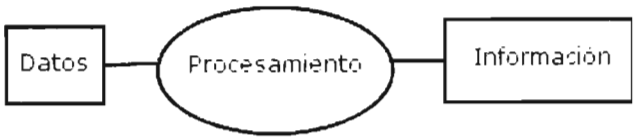


Fig.1.1.2. Formación de la información a partir de los datos.

Definición de sistema de comunicaciones

Podríamos definir a un sistema de comunicaciones como un conjunto de componentes encargados de transmitir información de un punto origen a un punto destino.

El propósito de un sistema de comunicaciones es transmitir información desde un emisor o fuente de la información hasta un destino a través de un canal.

Shanon definió que un sistema de comunicaciones consiste de cinco componentes, como muestra la Fig. 1.1.3:

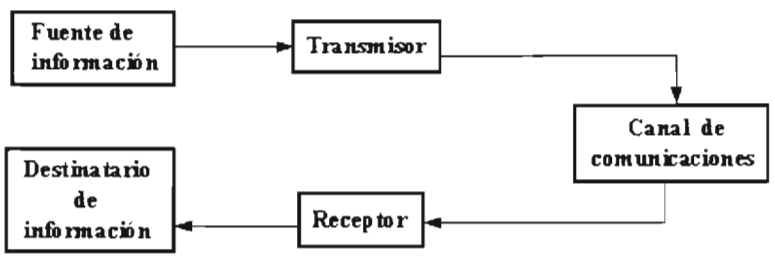


Fig. 1. 1.3 Componentes de un sistema de comunicaciones según Shanon

Estos componentes son:

1) Una fuente o emisor de la información. Es la parte del sistema que origina los símbolos o el mensaje a transmitir, este mensaje puede ser del tipo voz, video, datos.

2) El transmisor. Un transmisor de información cuya función es depositar la información de la fuente en un canal de comunicaciones, pasa la información en forma de señal. Es el que se encarga de hacer diferentes adecuaciones a la señal para poder trasmitirla en una forma optima, como por ejemplo digitalizar la señal o modularla para acoplar la señal transmitida a las propiedades del canal por medio de una onda portadora. Aquí el transmisor se encuentra en forma de bloque, pero representa o engloba a componentes como el codificador, el modulador preacentuador, muestreador, cuantificador, etc.

3) El canal. Un canal de comunicaciones a través del cual se hace llegar la información de la fuente al destino. Es el medio a través del cual la fuente envía la señal hasta el receptor, este medio puede ser: físico como un par de alambres, cable coaxial, fibra óptica; no físico como las ondas de radio, satélites y microondas u otros avances tecnológicos. Todos estos medios se caracterizan por tener una atenuación que es la disminución progresiva de la potencia de la señal conforme aumenta la distancia.

El termino canal puede tener los siguientes significados en telecomunicaciones:

1. Es una conexión entre los puntos de inicio y terminación de un circuito.
2. Es un camino único facilitado mediante un medio de transmisión que puede ser:
   a) Con separación física como un par de cable multipares.
   b) Con separación eléctrica como la multiplexión por división de frecuencia MDF o por división de tiempo TDM.
3. Es un camino para el transporte de señales eléctricas o electromagnéticas.

4) El receptor. Un receptor que tiene la función de extraer la información del canal y entregarla al destinatario. Extrae la señal del canal y la entrega al transductor de salida, debe tener varias etapas de amplificación. Es la contraparte del transmisor ya que se encarga de deshacer las modificaciones que pudo haber hecho el transmisor y puede por lo tanto demodular la señal, decodificarla hasta convertir la señal recibida a su forma original o a una señal eléctrica que pueda ser manejada por el destino. El receptor esta en forma de bloque pero engloba al demodulador, decodificador, filtro, desacentuador, etc.

5) El destino. El componente del sistema de comunicaciones al que va dirigida la información. Es la contraparte de la fuente, a la que se quiere hacer llegar la información.

El problema y objetivo central de las telecomunicaciones es hacer llegar la información que genera la fuente en un punto geográfico hasta el destinatario de la manera más rápida (para que la información no pierda su importancia), en forma segura (para que la información no caiga en manos de alguien que haga mal uso de ella o a quien no estaba destinada), veraz (para que el proceso de transmisión no altere el contenido de la información) y económica (tratando de mantener los costos que implica el proceso reducidos.)
El sistema obtiene la información de una fuente y la hace llegar al destinatario por medio de un mensaje a través de un canal de comunicación, el destinatario esta separado de la fuente desde unos pocos centímetros hasta miles de kilómetros.

¿Qué es un Mensaje?
Un mensaje no es lo mismo que la información. Un mensaje contiene a la información, se usa el mensaje para hacer llegar la información de la fuente al destino, el mensaje es la codificación de la información.
Los mensajes pueden ser de dos tipos digitales o analógicos. Los digitales se constituyen con un número finito de valores.
Los analógicos se constituyen con un número infinito de valores que varían en un rango continuo.

El ruido, elemento intrínseco de los sistemas de comunicaciones.
El ruido es un elemento muy importante en los sistemas de comunicaciones, por lo que representar un sistema de comunicaciones incluyendo al ruido lo hace más representativo como muestra la Fig. 1.1.4

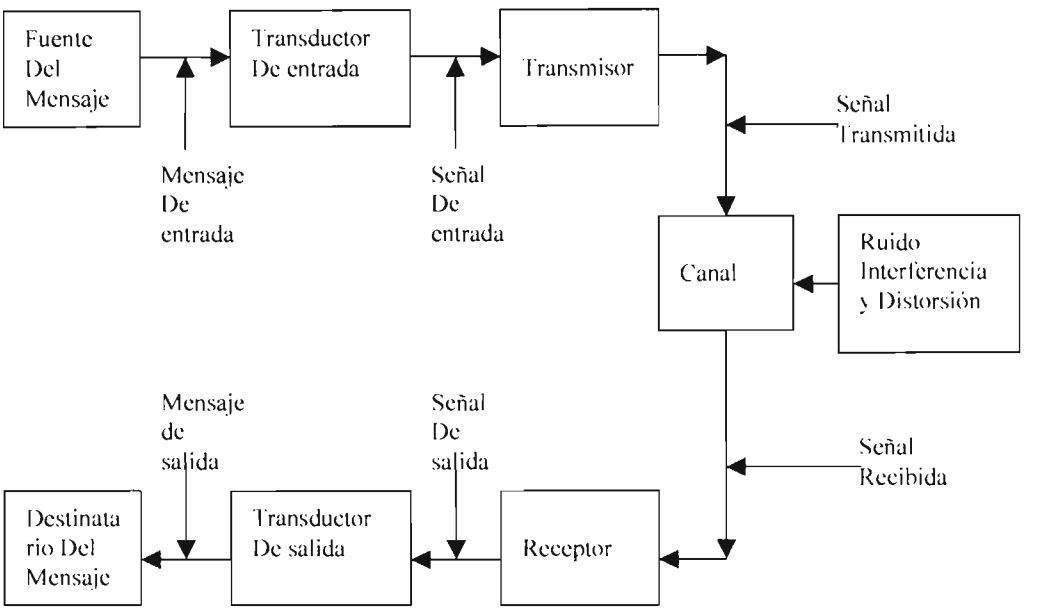


Fig. 1.1.4 Representación de un sistema de comunicaciones incluido el ruido

En la Fig. 1.1.4 tenemos un sistema de comunicaciones mas detallado e incluyendo el ruido, los componentes que se han agregado en este esquema son:

- El transductor de entrada. Convierte o transforma la señal original a otro tipo de señal para que pueda ser transmitida por el medio como por ejemplo, una señal eléctrica.
- El transductor de salida. Regenera la señal a su forma original como fue creada por la fuente para que sea interpretada por el sistema destino.
- Ruido y distorsión. Estos dos agentes se representan como elementos de un sistema de comunicaciones debido a que siempre están presentes en el, no porque se requieran o se hayan puesto ahí, sino por que son intrínsecos a los componentes. La distorsión es creada por una parte por la atenuación de la señal en el canal y por ruidos de diferentes tipos que se introducen en el sistema, como el ruido impulsivo, ruido térmico, etc. Junto con estos dos agentes tenemos otras imperfecciones en los canales como el tiempo de propagación, función de transferencia de canal no lineal, caídas súbitas de la señal, limitaciones en el ancho de banda y reflexiones de señal o eco.

  En las transmisiones analógicas se tiene el grave problema de la incorporación de ruidos durante el proceso de emisión-recepción que hace que la señal se altere o transforme en el camino. Este problema es una de las mayores desventajas de las comunicaciones analógicas.
- El mensaje. El mensaje puede ser de dos tipos mensaje analógico o mensaje digital.

El proceso de comunicación necesita de un agente emisor y de un agente receptor, los cuales pueden ser personas o medios mecánicos o electrónicos; y de un canal de información a través del cual se establezca la comunicación.

El proceso de mover información de un lugar a otro se conoce como transmisión. La información que puede transmitirse es variable: desde la voz humana, hasta datos provenientes de una computadora o imágenes de televisión. Esta información viaja en forma de señal eléctrica, la cual puede ser analógica o digital.

1.2 Características de las señales en los sistemas de comunicación

Así como los sistemas tienen gran importancia en la información y en las telecomunicaciones las señales también son de gran importancia en el estudio de las comunicaciones.
Las señales son de diferente naturaleza dependiendo de la fuente que las genera, por ejemplo podemos tener señales en acústica generadas por fuentes de sonido como la voz la música u otro ruido; señales de tipo térmico, mecánico o eléctrico en control de procesos en medicina pueden ser señales eléctricas o magnéticas generadas por el organismo humano, en sismología señales mecánicas.
Todas las señales independientemente de su fuente tiene algo en común: cada una tiene una o más características que reflejan el comportamiento de uno o varios fenómenos físicos, es decir alguna de las características de la señal contiene información de un fenómeno físico.

Concepto de señal
Una señal es una función de una o más variables físicas que transportan información de la naturaleza o comportamiento de algún fenómeno, estas señales tienen una representación en forma eléctrica. Las señales se propagan por el medio de comunicación y en sus variaciones va contenida la información codificada como datos.
Una señal tiene una gran dependencia del tiempo lo cual es una de las características más importantes de casi todas las señales. Por eso se dice que las características de la señal son función del tiempo como se muestra en la Fig. 1.2.1:

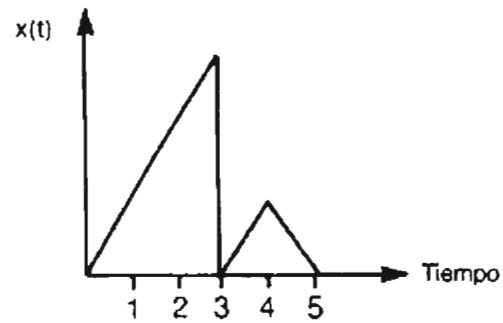


Fig. 1.2.1 Señal en función del tiempo

En la Fig. 1.2.1 tenemos una señal en función del tiempo x (t).
Donde:

- x indica la amplitud de la señal.
- t representa el tiempo.

Una señal tiene tres características básicas: el tiempo, la amplitud y la frecuencia. Estas características o parámetros de la señal se muestran en la Fig.1.2.2.

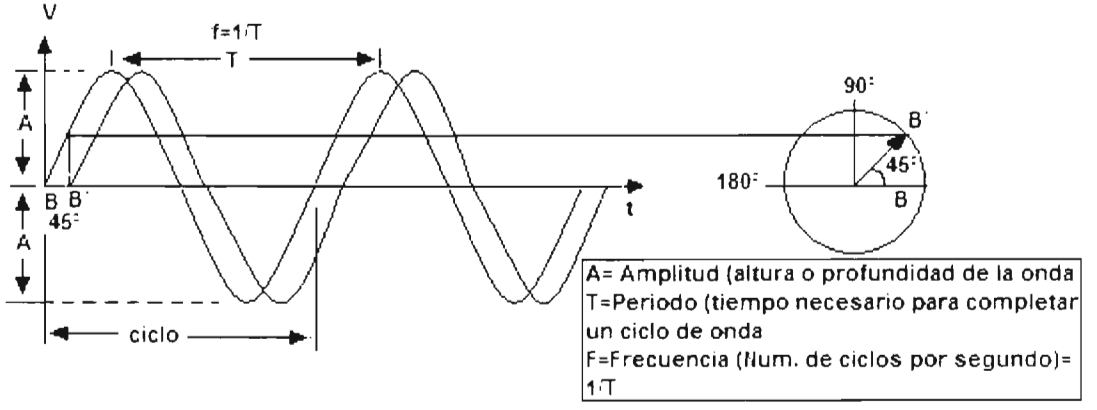


Fig.1.2.2 Parámetros característicos de una señal

Los parámetros que componen a la señal de la Fig. 1.2.2, son:

1. Amplitud. Es el valor máximo que toma la señal en el tiempo.
2. Frecuencia. Este parámetro indica la velocidad de repetición de un fenómeno periódico. Es él número de veces que se repite la señal (ciclos completos) por unidad de tiempo. La unidad de medida es el Hertz (hz.=ciclos por segundo), 1 hz. es un evento (ciclo) que tiene lugar una vez por segundo. Entendiéndose por ciclo la repetición de un evento, dicho evento esta conformado por una cresta positiva y una negativa. Los múltiplos de la frecuencia son Khz. (1000 ciclos por segundo), MHz (1000000 ciclos por segundo) y GHz (mil millones de ciclos por segundo), alternativamente la frecuencia se puede definir como el inverso del tiempo entre dos ocurrencias de ciclo (periodo), así:

f=1/T

Donde el periodo T esta dado en segundos.

3. Periodo. Es el tiempo requerido para que se complete un ciclo completo de una señal, o también se puede obtener de la medición del tiempo entre dos ocurrencias de ciclo. Por otra parte se puede obtener del inverso de la frecuencia.

T=1/f

4. Fase. Mide la posición relativa de la señal y se mide en radianes

Tipos de señales

Las señales se pueden clasificar en forma genérica como:

- Señales continuas o analógicas
- Señales discretas o digitales
- Señales periódicas
- Señales no periódicas

Señales continuas

Una señal x (t) es continua si esta definida para todo el tiempo t, es decir

Lim t→a x(t) = x(a)

La señal varía suavemente en el tiempo sin discontinuidades, por Ej. la voz.

- **Señales analógicas o continuas en amplitud**

Estas son las señales que varían de una forma continua en función del tiempo, conforme avanza el tiempo la señal adquiere valores dentro de un intervalo continuo. Son señales continuas tanto en el tiempo como en amplitud como muestra la Fig. 1.2.3.

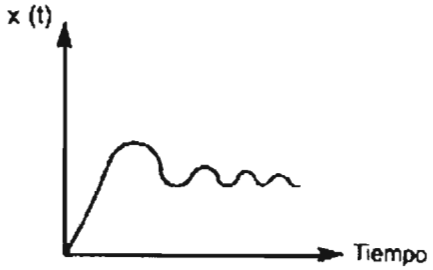


Fig. 1.2.3 Señal x (t) continua en el tiempo y continua en amplitud

El gran problema con estas señales es la atenuación que se produce con la distancia por lo que se tienen que usar amplificadores, esta amplificación provoca que el ruido que se introduce en las señales se amplifique también empeorando la calidad de la señal en la recepción.

- **Señales analógicas continuas en tiempo, discretas en amplitud**

Estas señales solamente toman ciertos valores a lo largo del tiempo como muestra la Fig. 1.2.4.

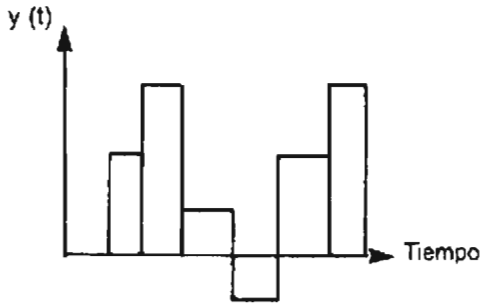


Fig. 1.2.4 Señal y (t) continua en el tiempo, discreta en amplitud

Señales discretas

Una señal discreta es una secuencia de números identificada como x(n) donde n es un número entero. Una señal discreta se puede obtener al hacer un muestreo de una señal continua. Representa solo los valores en algunos instantes de tiempo, es decir mantiene un valor constante cierto tiempo tras lo cual pasa a otro valor de forma discontinua.

- **Señales digitales discretas en el tiempo y discretas en amplitud**

Son señales discretas en el tiempo y discretas en amplitud por que adquieren ciertos valores de un conjunto finito de símbolos únicamente en ciertos instantes de tiempo. Estas señales son obtenidas mediante técnicas de muestreo que ayudan a digitalizar a las señales analógicas. Este tipo de

señales son de gran importancia en las comunicaciones digitales ya que los sistemas de telecomunicaciones son eficientes y efectivos gracias a estas señales. Esta señal se muestra en la Fig. 1.2.5.

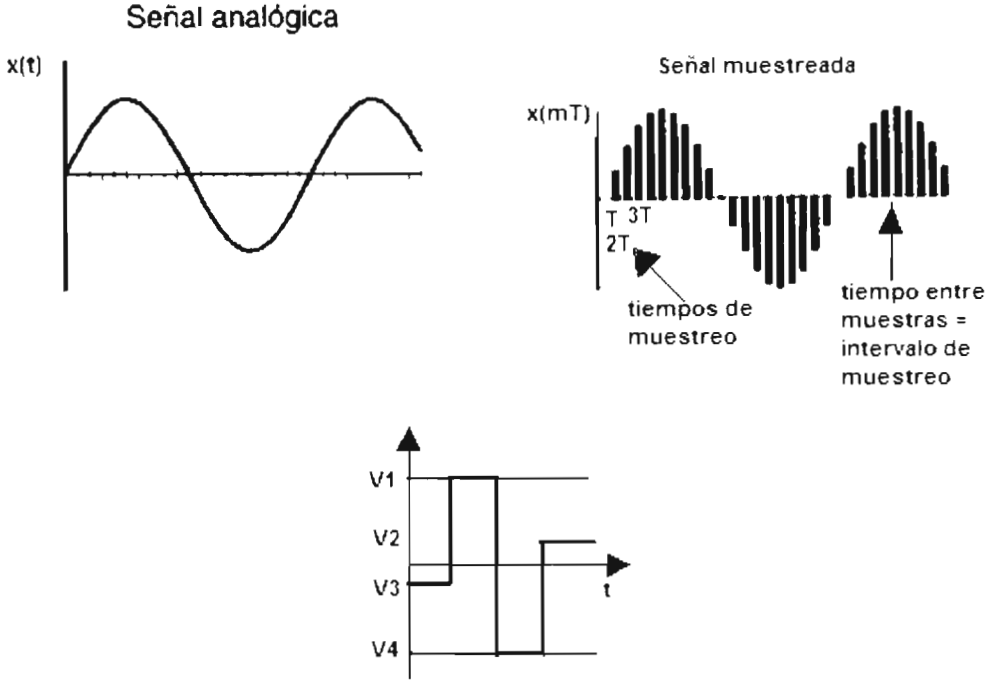


Fig. 1.2.5 Señal Digital = Señal analógica x (t) y su versión muestreada x (mT)

Las muestras ocurren en los instantes en que el tiempo t toma los valores T, 2T, 3T,...etc. Este tipo de señales son secuencias de pulsos de voltaje. Con este tipo de señales se elimina el problema de la perdida de calidad pues en lugar de amplificadores se usan repetidores. Los repetidores no solo aumentan la potencia de la señal sino que también decodifican los datos y los codifican de nuevo regenerando la señal en cada salto, con lo cual el enlace podría tener longitud infinita.

- **Señal digital binaria**

La señal digital binaria es una señal discreta en el tiempo y en amplitud. Señal cuya amplitud únicamente toma valores de dos símbolos el 0 y el 1. Fig.1.2.6.

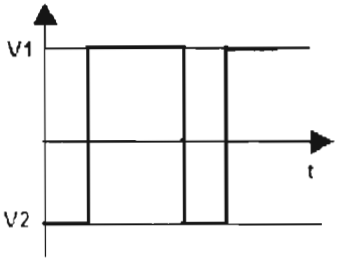


Fig. 1.2.6 Señal digital binaria

- Señales senoidales. Aunque están dentro de las analógicas, por su importancia en el estudio y análisis de señales hacemos mención de ellas aparte, ya que se usan para estudiar la manera en que transportan la información las señales o para modelar el comportamiento de cualquier otra señal.

Una señal senoidal es una onda con una sola frecuencia, tiene una representación matemática de la siguiente forma:

$Z(t)=a(t)$ sen wt

Donde:

- a(t) es la amplitud de la señal si a(t) es constante a(t)=a.
- sen es la función trigonométrica del seno.
- t es el tiempo.
- w es la frecuencia de la señal que se mide en hertz, la cual representa la variación de un ciclo completo de la señal en un segundo.

En la figura 1.2.7 se observan 3 señales senoidales con diferentes frecuencias

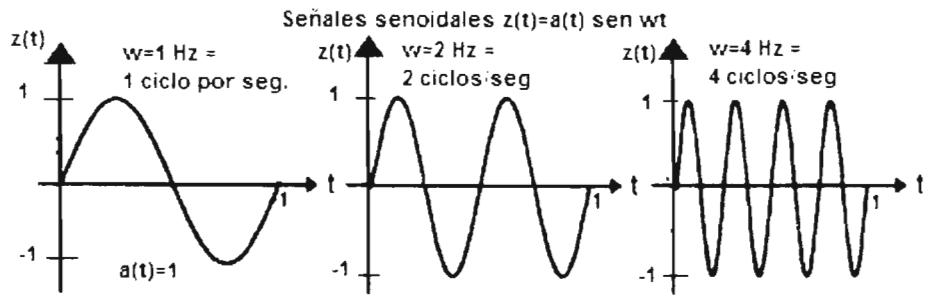


Fig. 1.2.7 Señales senoidales con diferentes frecuencias

Aparte de su interés matemático las señales senoidales son muy importantes por que en condiciones generales muchas señales pueden ser expresadas como una suma de ondas o señales senoidales, como se ve en la Fig. 1.2.8

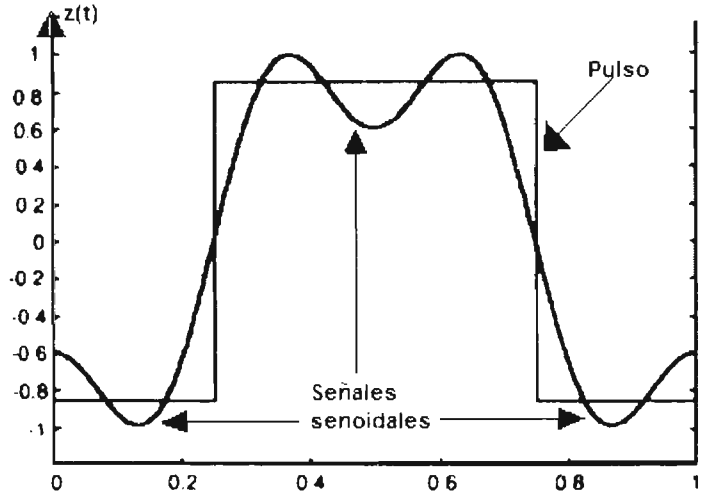


Fig.1.2.8 Un pulso representado como una suma de senoides. Esto fue establecido por J. Fourier

- **Señales periódicas**

Estas señales se caracterizan por que se repiten a lo largo del tiempo o se repite un cierto patrón en el tiempo de tal manera que se cumple la siguiente condición:

$g(t)=g(t+To)$ para $To\neq 0$

Donde:

- To es el periodo fundamental de una señal.
- f es la frecuencia fundamental y se mide en hertz, es el inverso del periodo $f=1/T$
- $w=2\P/T$ es la frecuencia angular y se mide en radianes por segundo

Una señal periódica se conserva sin cambio al aplicársele un corrimiento positivo o negativo de cualquier entero múltiplo del periodo To, esto se cumple para $-\infty<t<\infty$
Si se cumple la condición $g(t)=g(t+To)$ para $To\neq 0$ la señal es periódica con periodo T, como muestra la Fig. 1.2.9.

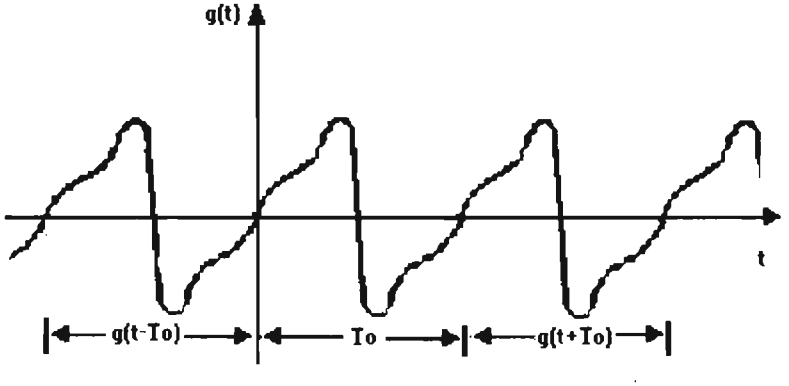


Fig. 1.2.9 Señal Periódica

Como ejemplos de señales periódicas podríamos tener a las señales senoidales y los trenes de pulsos. Las señales analógicas y digitales pueden ser periódicas como muestran la Fig. 1.2.10 y la Fig.1.2.11

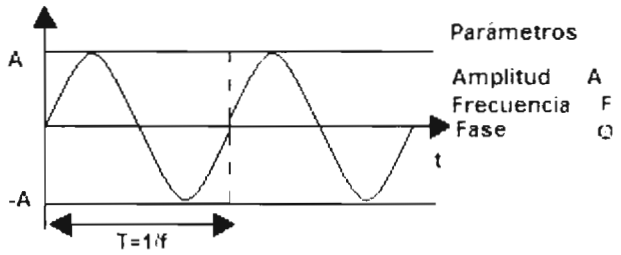


Fig. 1.2.10 Señal Analógica Periódica X (t)=A_i cos (2¶f_it+φ_i)

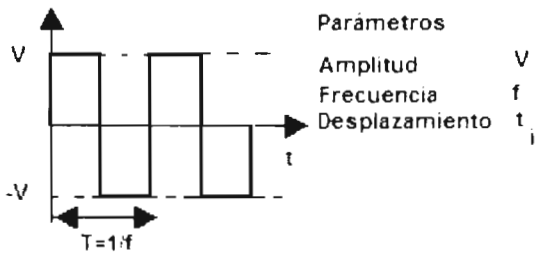


Fig. 1.2.11. Señal digital periódica X(t)=V 0<t<T/2, X(t)=-V T/2<t<T

- **Señales no periódicas**

Son aquellas señales cuyo valor del periodo es infinito. También en este caso las señales analógicas y digitales pueden ser no periódicas como muestran la Fig. 1.2.12 y la Fig. 1.2.13

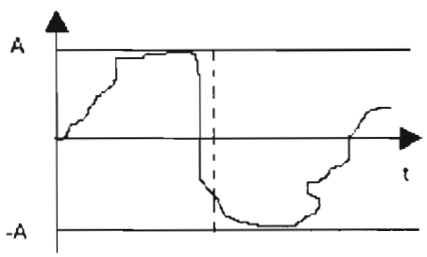


Fig. 1.2.12 Señal analógica no periódica

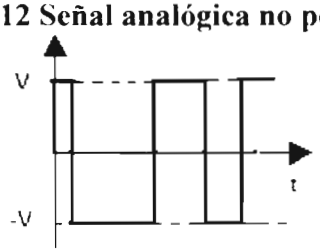


Fig.1.2.13 Señal digital no periódica

Representación de las señales

El estudio o análisis de señales se realiza representándolas o modelándolas en tres formas:

- Representación en el dominio del tiempo.
- Representación en el dominio de la amplitud.
- Representación en el dominio de la frecuencia o representación espectral. Se aplica a señales sinusoidales de la forma: $A_i \cos (2\P f_i t+\varphi_i)$.

A su vez la representación en el dominio de la frecuencia puede hacerse en dos formas:

- Representación espectro de amplitud.
- Representación espectro de fase.

- **Representación en el dominio del tiempo**

El análisis en el dominio del tiempo es el dominio primario en el que se manejan y captan las señales, este tipo de representación se describe en función del tiempo de la siguiente forma:

Cos (wt+φ) ó e^{-at}

Con números complejos x (t)+iy (t)

Como se puede ver la señal depende de la variable tiempo.

El dominio del tiempo nos permite conocer parámetros de la señal como el valor de pico, valor de pico a pico, valor medio, valor medio cuadrático, la varianza o factor de forma.

- **Representación en el dominio de la amplitud**

El análisis de las señales en el dominio de la amplitud permite determinar propiedades estadísticas de las señales.

- **Representación en el dominio de la frecuencia**

Para representar las señales en el dominio de la frecuencia, estas se modelan como una suma de diferentes frecuencias, estas frecuencias son los espectros de las señales periódicas los cuales toman valores a las frecuencias de 0, fo, 2fo..... nfo

- Representación del espectro de amplitud

En esta representación de las señales sé grafica la amplitud contra la frecuencia como se observa en la Fig. 1.2.14.

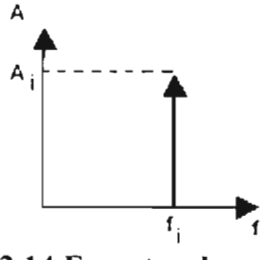


Fig. 1.2.14 Espectro de amplitud

- Representación espectro de fase

El espectro de fase representa la fase de la señal contra la frecuencia. Fig. 1.2.15

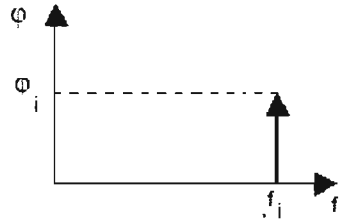


Fig. 1.2.15 Espectro de fase

Análisis de las señales

El estudio de las señales es más sencillo en el dominio de la frecuencia. Normalmente tenemos las señales en el dominio del tiempo por lo que se puede realizar una transformación del dominio del tiempo al dominio de la frecuencia para evaluar como se distribuye la energía en función de la frecuencia.

Las señales se estudian sobre la base del teorema de Fourier el cual a su vez se basa en el estudio del movimiento ondulatorio. El movimiento ondulatorio se representa mediante la ecuación general x=g (t).

Teorema de Fourier

El teorema enuncia que cualquier señal se puede descomponer en una suma de señales periódicas

Análisis de señales periódicas

El teorema de Fourier se puede aplicar al análisis de las señales periódicas de la siguiente forma:

Una función periódica x (t) se puede representar como una combinación lineal de funciones senos y cosenos.

El análisis de Fourier describe las señales periódicas sobre la base de las propiedades de las componentes armónicas cos (mw_0t) y sen (mw_0t). Donde las frecuencias armónicas mw_0t son múltiplos enteros de la frecuencia fundamental w_0.

El análisis en el dominio de la frecuencia descompone la señal en las frecuencias que la componen representando las señales periódicas mediante su desarrollo en serie de Fourier y las no periódicas mediante la transformada de fourier. de aquí se obtiene una análisis espectral ya que se representa la señal mediante su espectro de frecuencias.

Las señales periódicas se pueden representar mediante una serie de fourier o mediante una serie exponencial de fourier.

Representación de una señal periódica mediante la serie de fourier

La serie trigonométrica de Fourier representa una señal continua como la suma de todas las componentes posibles. senos o cosenos para todas las frecuencias armónicas.

Sea una señal periódica que cumple con la condición:

$g(t)=g(t+To)$ para $To\neq 0$

Esta señal periódica puede ser representada como una serie trigonométrica de fourier que no es otra cosa mas que la suma de senoides de frecuencias 0, fo, 2fo,..., kfo
donde fo es la frecuencia de repetición y se define como fo=1/To
Así la expresión espectral de la serie trigonométrica de Fourier es:
$G(t)=a_o+\sum_{n=1}^{k}(a_n\cos 2\P nf_ot+ b_n \text{ sen } 2\P nf_ot)$

Donde:

- a_o es el coeficiente de componente coseno de frecuencia cero, esto es es la componente de corriente directa o constante de la señal. Dicho de otra forma es el valor promedio o componente continua de la señal. Se determina con la siguiente formula: $a_o = (1/T)\int_{to}^{to+To} g(t)\,dt$
- fo es la frecuencia de repetición que es inversamente proporcional al periodo To.
- $w_o=2\P f_o=2\P/T_o$ es la frecuencia fundamental.
- $nw_o= n2\P f_o$ son las frecuencias armónicas.
- a_n son los coeficientes de Fourier de los cosenos o amplitudes, se definen de la siguiente forma: $a_n=(2/T_o)\int_{to}^{to+To} g(t)\cos nw_ot\,dt$
- b_n son los coeficientes de Fourier de los senos o amplitudes se determinan con la formula: $b_n= (2/T_o)\int_{to}^{to+To} g(t)\text{ sen } nw_ot\,dt$

Esta forma de representar una señal nos dice que cualquier señal periódica g (t) con periodo T_o puede expresarse como una suma de senoides de frecuencias fo y todos sus enteros múltiplos ($f_o=1/T_o$)
La forma compacta de la serie de Fourier es:
$G(t)=C_o+\sum_{n=1}' C_n\cos(nw_ot+\Theta_n)$

Donde:

- $w_o=2\pi f_o$
- $C_o=a_o$
- $C_n=\sqrt{(a_n^2+b_n^2)}$
- $\Theta_n=-\tan^{-1}(b_n/a_n)$

La serie de fourier nos permite obtener las graficas del espectro de magnitud (c_n vs w) y del espectro de fase (Θ_n vs w).
Así como se pueden representar las señales como series trigonométricas de fourier también se pueden representar como una serie exponencial de fourier:
$g(t)=\sum_{n=-\infty}' G_ne^{jnwot}$

Donde:

- $w_o=2\P f_o=2\P/T_o$
- Los coeficientes complejos Gn se obtienen con la integral
  $G_n=(1/T_o)\int_{to}^{to+To} g(t)e^{-jnwot}dt$

Las series trigonométrica y exponencial de Fourier no son dos series diferentes, son dos formas distintas de representar la misma serie.

Concretamente el teorema de fourier se interpreta como:
Una función periódica arbitraria se puede obtener sumando movimientos ondulatorios simples cuyos valores de frecuencias armónicas son múltiplos de una fundamental y cuyas amplitudes sean seleccionadas correctamente.
Por lo tanto las series de Fourier expresan que la señal g (t) puede escribirse como una combinación lineal de valores infinitos por lo cual se puede representar en el dominio de la frecuencia en la forma de espectro en rayas, estando estas líneas espectrales situadas sobre valores de frecuencias que son múltiplos enteros de la fundamental.
En realidad el método lo que hace es superponer los movimientos ondulatorios armónicos a la forma que tiene el movimiento periódico en cuestión.

Representación de señales no periódicas
El método de fourier se aplica también a señales no periódicas con solo suponer que la señal se extiende en el infinito y que este intervalo corresponde a un solo periodo. En este caso en lugar de analizar la curva en un espectro discreto de frecuencias w, 2w, 3w,..... nw se analiza en un espectro continuo.
Las señales no periódicas se pueden representar con una suma continua de señales exponenciales eternas mediante la transformada de Fourier.
Esta forma de representación parte de una función no periódica g(t), la cual se representa primeramente como una suma continua de funciones exponenciales eternas con frecuencias que están en el intervalo $-\infty<w<\infty$. Así:
g (t) es la señal no periódica

$g(t)= (1/2¶) \int_{-\infty}^{\infty} G(w)\, e^{jwt} dw$ representa a g(t) como una suma de funciones exponenciales eternas
$g(w)= \int_{-\infty}^{\infty} g(t)\, e^{-jwt} dt$ representa el espectro de frecuencias de g (t) el cual es continuo

Entonces g (w) es la transformada de Fourier de g (t)
$g(w)= \int_{-\infty}^{\infty} g(t)\, e^{-jwt} dt$

A su vez g (t) es la transformada inversa de fourier de G (w)
$g(t)= (1/2¶) \int_{-\infty}^{\infty} G(w)\, e^{jwt} dw$

La transformada de fourier es el elemento básico para representar una señal en términos de sus componentes exponenciales de diferentes frecuencias. Así se tienen dos formas de describir una misma función en el dominio del tiempo y en el dominio de la frecuencia.
En síntesis las señales continuas se componen por muchas frecuencias de una señal seno. Si todas las frecuencias son múltiplos de una frecuencia dada, esa frecuencia es la frecuencia fundamental.
El espectro de una señal es el conjunto de frecuencias que constituyen la señal.
El ancho de banda es la anchura del espectro. Muchas señales tienen un ancho de banda infinito, pero la mayoría de la energía esta concentrada en un ancho de banda pequeño.
Si una señal tiene una componente de frecuencia 0, es una componente continua.

1.3 Transmisión de información

Uno de los principales objetivos de los sistemas de comunicación es la transmisión de la información, esta transmisión de información depende de la capacidad de transmisión de dichos sistemas. Los sistemas de comunicación tienen en el ancho de banda y el ruido dos de los elementos más importantes que influyen en el logro de una transmisión eficiente. En este tema definiremos algunos conceptos relacionados a la transmisión de la información, como ancho de banda, velocidad, capacidad de transmisión, capacidad de los canales, potencia de señales y ruido.

Transmisión
La transmisión es la comunicación de los datos mediante la propagación de señales a través del medio. La transmisión puede ser analógica o digital dependiendo del tipo de señal que se propague en el medio para transmitir la información.

Canal de transmisión
El canal de transmisión es la vía de comunicación física del sistema de comunicaciones necesaria para que una señal de tipo eléctrica, óptica o electrooptica se pueda desplazar del transmisor al receptor. Este canal puede ser analógico o digital.
El canal es analógico cuando la señal que se transmite a través del canal es analógica, este canal se caracteriza por su ancho de banda en ciclos por segundo Hertz (hz.), el canal de transmisión analógico también puede transmitir señales digitales previamente moduladas.
El canal es digital si transmite una señal digital caracterizado por la capacidad en bits por segundo (bps), también transmite señales analógicas previamente digitalizadas.
Los siguientes elementos influyen en la capacidad de transmisión de un canal:

- Ancho de banda del canal y de la señal
- Velocidad de transmisión de datos
- Atenuación
- Distorsión
- Ruido
- Relación señal/ruido
- Técnicas de modulación y codificación

Ancho de banda del canal
Cada medio de transmisión tiene un límite superior e inferior para las frecuencias que puede transmitir, este rango limitado de frecuencias que se pueden transmitir con fidelidad por el medio es el ancho de banda. Un sistema digital maneja la capacidad o régimen binario el cual es definido por el número de bits por segundo, este régimen binario es proporcional al ancho de banda disponible, el ancho de banda se puede calcular de la siguiente manera:

BW = Frecuencia Máxima-Frecuencia Mínima
Donde BW=ancho de banda por sus siglas en ingles, se mide en Hertz (hz.)
Así por ejemplo el cable telefónico tiene las frecuencias mínima y máxima de 300 hz. y 3700 hz.
Por lo tanto su ancho de banda es BW=3700-300 = 3400 hz.
Aunque normalmente se usa la máxima frecuencia para referirse al ancho de banda.

Por su parte el ancho de banda digital es la cantidad o volumen de datos que se pueden enviar a través de un canal, medidos en bits por segundo (bps).
No se debe confundir las unidades de expresión Mhz con Mbps, aunque ambas unidades se usan para expresar la velocidad de transmisión.
Así la velocidad en bits expresa la cantidad de bits que se pueden transmitir por un canal y depende de la aplicación que se usa así como de ciertas técnicas como por ejemplo la codificación de la información.
La unidad de expresión hertz tiene una relación proporcional o polinomial con el BIT rate, si se usan diferentes sistemas de codificación, diferentes BIT rates se pueden relacionar con el mismo numero de ciclos por segundo o Hz.
De esta manera dependiendo de la codificación utilizada, el flujo de información ocupara una señal con un ancho de banda definido. Por ejemplo el estándar ethernet a 100 Mbps (Fast ethernet) con codificación 5B6B requiere un BW de 25 MHz, pero cuando se usa una codificación de 4B5B se requerirá un BW de 31.25 MHz.
Por lo tanto es mas adecuado expresar la velocidad en MHz, puesto que se habla de la velocidad real del enlace, el bit rate dependerá de la codificación.

Velocidad de transmisión de datos
La velocidad de transmisión puede estar dada en bits por segundo (bps) o en baudios que es el numero de cambios por segundo que experimenta una señal.
La velocidad de transmisión es mayor tanto mayor sea el ancho de banda, y si la velocidad de transmisión es mayor el ancho de banda debe ser mayor para tener la capacidad de transmitir a esa velocidad mayor. Esta relación entre la velocidad de transmisión y el ancho de banda es debido a que el medio de transmisión limita las componentes de frecuencia a las que puede ir la señal, por ejemplo en el caso de una onda cuadrada que se pueden simular con la suma de múltiplos impares de la frecuencia fundamental de ondas senoidales, cuando mas ancho de banda se tenga mas se asemeja la función seno a la onda cuadrada.

Ancho de banda de la señal
El ancho de banda de una señal es el rango de frecuencias en el que esta contenida la mayor parte de la energía de una señal, se expresa en unidades de Hertz (Hz.).

Atenuación
La atenuación es la disminución de potencia o amplitud de una señal provocada por la perdida de energía en su paso a lo largo de la trayectoria del canal, esta perdida de potencia puede ser mínima para distancias pequeñas hasta de proporciones muy importantes para grandes distancias como la comunicación interplanetaria. La atenuación que sufre una señal dependerá mucho de la frecuencia. Para poder subsanar esta atenuación se tiene que regenerar la señal mediante amplificadores, estos equipos restauran la energía perdida a la señal para que su amplitud sea nuevamente manejable.
La atenuación se puede calcular de la siguiente forma:
$A=10\log_{10}(P_T/P_R)$
Donde:

- P_T es la potencia de transmisión.
- P_R es la potencia de recepción.

La atenuación se representa en unidades de decibeles por metro dB/m

Distorsión

La distorsión es el efecto de transmitir una señal de mayor ancho de banda por un canal con un ancho de banda menor, este efecto se ilustra en la Fig. 1.3.1

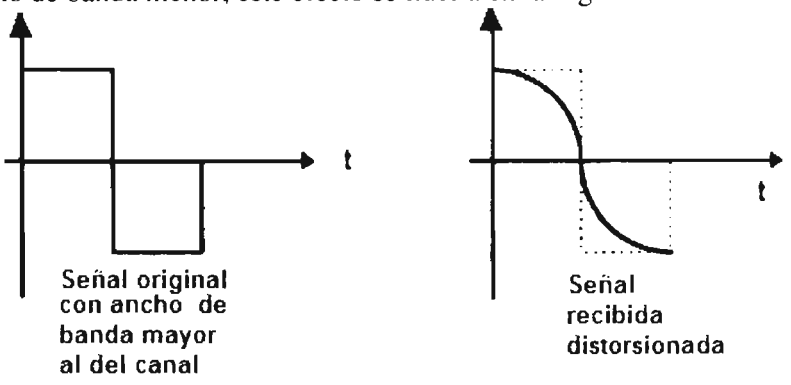


Fig. 1.3.1 Distorsión por anchos de banda diferentes

La distorsión también puede ser provocada por la atenuación y los corrimientos de fase de las componentes de frecuencia de la señal, por lo que las diferentes componentes de la misma señal llegan en instantes diferentes al receptor, provocando que el pulso se redondee siendo esta una distorsión lineal. Pero puede ser que la atenuación varié con la amplitud de la señal lo que se conoce como distorsión no lineal.

Un ejemplo de distorsión se puede ver si se transmite música de alta fidelidad de 20 Khz, por el canal telefónico de 4 Khz., la música se escuchara diferente debido a la distorsión.

Las señales digitales son un caso importante por su ancho de banda infinito. Estas señales se deben acotar en frecuencia debido al ancho de banda y a la limitación del medio de transmisión. Al eliminar frecuencias de la señal en el tiempo se produce una distorsión, o sea nunca obtendremos pulsos perfectos sino aproximaciones, lo cual dificulta la recepción. Así cuanto mayor es la limitación en frecuencia mayor es la distorsión y mayor la probabilidad de error.

Interferencia

La interferencia se presenta en la transmisión cuando se adiciona una señal conocida y no deseada que se superpone a la señal original.

En los sistemas digitales tenemos la interferencia entre símbolos o bits lo cual es uno de los factores que tiende a reducir la capacidad que puede alcanzar un canal, este tipo de interferencia se da por la limitación del ancho de banda del canal lo cual hace que al transmitir un pulso rectangular se redondeen las esquinas del pulso generando un sobredisparo de la señal de salida, esta prolongación de la señal de salida interfiere con los pulsos anterior y posterior lo que provoca que se malinterprete la señal, esto se muestra en la Fig. 1.3.2

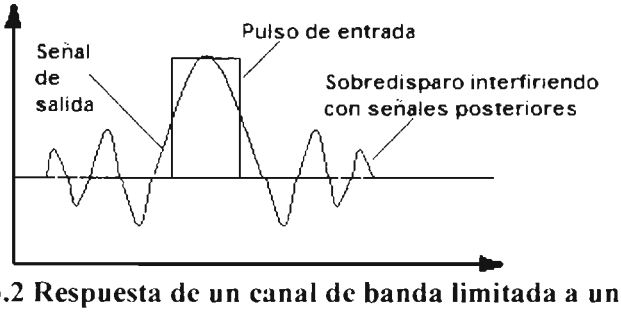


Fig. 1.3.2 Respuesta de un canal de banda limitada a un pulso

Potencia de la señal

La potencia de transmisión de las señales tiene doble función en la transmisión de la información. Primeramente su influencia en la calidad de la transmisión ya que al aumentarse la potencia S de la señal se reduce el efecto del ruido del canal y la información se recibe con mayor exactitud. Por otra parte una relación señal a ruido S/N mayor permite la transmisión a una distancia mayor. De cualquier manera la relación S/N siempre deberá ser mínima para la correcta comunicación. Una representación grafica de la relación S/N se encuentra en la Fig. 1.3.3.

Fig. 1.3.3 Relación señal a ruido

La potencia de las señales es referida en unidades de decibel dB.
Un decibel es la décima parte de un Bel el cual es la unidad de referencia para medir la potencia de una señal o intensidad del sonido también. Los logaritmos son empleados para describir la señal en dB. Así la ganancia de potencia en decibeles es:
$G'(dB)=10*\log_{10}(G)$
Donde:

- G´= ganancia de potencia en decibeles.
- G=ganancia de potencia sin unidades.

Los decibeles se transforman a unidades absolutas con la siguiente formula:
$P=10^{x/10}$
Donde x esta en decibeles
A veces los decibeles se usan para indicar el nivel de potencia respecto a 1 mW para lo cual se usa el simbolo dBm y se obtiene con la siguiente formula:
$P'=10\log(P/1mW)$
Donde:
- P´=potencia en dBm
- P=potencia en watts.

Ruido

El ruido es el conjunto de todas las señales aleatorias no predecibles e indeseables que contaminan a la señal transmitida. El ruido es considerado el principal enemigo de las comunicaciones ya que limita la identificación correcta de la señal y por tanto de la información transmitida, el ruido puede ser visto como una interferencia de origen desconocido y naturaleza aleatoria.
El ruido es inevitable en los sistemas de comunicaciones, ya que el simple movimiento de electrones genera ruido por lo que el propio sistema en si es un generador de ruido interno aunado a otros ruidos externos como las interferencias de otras señales vecinas.
En los sistemas de comunicación se tienen diferentes tipos de ruido, como el ruido blanco y los ruidos impulsivos.
Normalmente se procura que la variación de ruido sea muy pequeña para que pueda ser ignorado dependiendo de la relación de la señal transmitida al ruido. La relación señal a ruido se determina de la siguiente forma:
$S/N=10\log_{10}(P_S/P_N)$ expresada en decibeles.

Donde:

- P_S es la potencia de la señal.
- P_N es la potencia del ruido.

Tipos de ruido:

- Ruido Blanco, térmico o Gaussiano. Es el ruido introducido en la señal debido a la agitación de los electrones por efecto de la temperatura, es uniforme en el espectro (ruido blanco), este tipo de ruido no se puede evitar ni mucho menos eliminar.
- Ruido de inter modulación. Es el ruido generado cuando distintas frecuencias comparten el mismo medio de transmisión, es el ruido que aparece en sistemas no lineales, lo que provoca la aparición de nuevas frecuencias, estas nuevas frecuencias se suman o restan de las frecuencias de la señal original generando componentes frecuenciales que antes no existían y que distorsionan la señal original.
- Ruido de diafonía. El ruido de diafonía se produce cuando las señales viajan por medios adyacentes. Así la señal que viaja en una línea se acopla a la línea adyacente cercana distorsionando la señal que viajaba en esa línea, por ejemplo este se puede producir por acoplamiento de pares de cable cercanos o cuando antenas de microondas captan señales no deseadas.
- Ruido impulsivo. Este ruido a diferencia de los anteriores es impredecible, es un rumor continuo formado por picos irregulares de un poco duración y gran amplitud que afecta notablemente a la señal, en las comunicaciones analógicas este genera chasquidos breves y en las digitales transforma las ráfagas de bits provocando que se pierda toda la información. Es causante de muchos errores en la comunicación de datos. Se identifica como un clic en las comunicaciones de voz. Sus fuentes son los cambios de voltajes en líneas adyacentes, falsos contactos y arcos eléctricos en interruptores.

Capacidad de información del canal

La capacidad de un canal es la velocidad a la que se pueden transmitir los datos en un canal de comunicaciones de datos. La velocidad de los datos es la velocidad a la que se pueden transmitir estos en bits por segundo. El ancho de banda es el ancho de banda de la señal transmitida que se limita por el transmisor y la naturaleza del medio de transmisión en Hz.

La capacidad de información pone un límite máximo de transmisión de la información o velocidad de los sistemas de comunicación, este límite básicamente es provocado por los parámetros de ancho de banda y la relación señal a ruido. La capacidad será diferente en un canal sin ruido y en un canal con ruido.

Capacidad del canal sin ruido

Los canales digitales representan a los canales de este tipo, en este tipo de canales sin ruido la máxima velocidad de transmisión la impone el ancho de banda. Según Nyquist para un ancho de banda B dado si se transmiten señales binarias la mayor velocidad de transmisión es 2B, lo que a su vez es igual a la capacidad. Para el caso multinivel (transmisión con señales digitales) donde es posible codificar mas de un bit en cada ciclo es posible transmitir mas cantidad de información, por lo que tendremos:

Capacidad = $2B \log_2 M$

Donde: M es el número de niveles que se usa para codificar la señal.

Según la formula para aumentar la capacidad bastaría con aumentar el numero de niveles M, pero al aumentar los niveles estos están más próximos entre sí lo que aumenta el efecto del ruido. Al mismo tiempo si con cierto ancho de banda se intentara aumentar la velocidad de transmisión el ruido impulsivo afectaría a más bits, ya que al aumentar la velocidad los bits se comprimen en el tiempo.

Capacidad del canal con ruido

La capacidad de un canal con ruido Gaussiano, a través del cual se transmiten señales analógicas con un ancho de banda finito, es obtenida con la ecuación de Shannon:

$C=B*\log_2[1+(S/N)]$ bits/seg

Donde:

- C es la capacidad del canal en bps.
- B es el ancho de banda en hz.
- S/N es la relación señal a ruido en dB .

Para un ruido dado se puede aumentar la potencia de la señal S para aumentar la capacidad y la velocidad de transmisión, pero esto provocaría que los componentes no lineales se acentúen, así como el ruido inter modulación. Si se aumenta el ancho de banda B es la potencia de ruido blanco la que aumenta.

Como se puede ver la formula de Shanon nos proporciona una relación entre el ancho de banda B del canal y la velocidad de transmisión C.

El uso de sistemas eficientes de comunicación conduce a una reducción del tiempo de transmisión, esto es, se transmite mayor información en menor tiempo. Una transmisión rápida podría lograrse empleando señales que varían rápidamente con el tiempo, pero el sistema eléctrico cuenta con energía almacenada y una ley de la física dice que para todos los sistemas un cambio en la energía almacenada requiere una cantidad definida de tiempo, debido a esto si se incrementara la velocidad de la señalización en forma arbitraria el sistema dejaría de responder a los cambios de la señal.

La velocidad de una señal es su ancho de banda o ancho del espectro de la señal. Similarmente el régimen al cual puede un sistema cambiar energía almacenada se refleja en su respuesta útil medida por el ancho de banda del sistema. La transmisión de gran cantidad de información en poco tiempo requiere señales de banda ancha para representar la información y sistemas de banda ancha para acomodar las señales por lo que el ancho de banda es una limitación fundamental.

Para una transmisión en tiempo real se debe asegurar un adecuado ancho de banda del sistema, si este es insuficiente se debe disminuir la velocidad de señalización, incrementando por tanto el tiempo de transmisión. El diseño de un sistema no es con mucho un problema de ancho de banda absoluto fraccionario, o sea, el ancho de banda absoluto dividido entre la frecuencia central. Si con una señal de banda ancha se modula una portadora de alta frecuencia se reduce el ancho de banda fraccional.

Por lo tanto tenemos que en la transmisión a mayor ancho de banda mejor calidad y mayor velocidad con la que podemos transmitir información. El diseño de los sistemas de comunicación es un compromiso entre el tiempo de transmisión, potencia transmitida, ancho de banda y relación señal a ruido.

Tipos de transmisión

Los tipos de transmisión de un canal de comunicaciones pueden clasificarse de la siguiente forma:

Por el sentido de la transmisión.

- Simplex.
- Semiduplex.
- Duplex o duplex completo.

Por el modo de transmisión.

- Paralelo.
- Serie.

Por el formato de transmisión.

- Síncrono.
- Asíncrono.

- **Transmisión simplex**

En este sentido de transmisión simples un extremo siempre actúa como transmisor y el otro extremo siempre actúa como receptor, la transmisión es en un solo sentido por lo que se tiene un canal físico de comunicaciones y un canal lógico de comunicaciones, no es posible invertir los papeles, por lo que el transmisor siempre será transmisor y el receptor solamente será receptor, un ejemplo de este sistema es la transmisión de televisión, el aparato de TV siempre es el receptor y la antena siempre es el transmisor.

- **Transmisión semiduplex**

En la transmisión semiduplex en un momento dado un extremo es el transmisor y el otro el receptor y en otro momento el primero puede ser el receptor y el segundo el transmisor y así sucesivamente se intercambian los papeles según se tenga la necesidad de que uno u otro extremo sea el que transmita. La transmisión se puede realizar en los dos sentidos pero no al mismo tiempo como una conversación de radioaficionados donde uno espera a que el otro termine de hablar para continuar el dialogo.

- **Transmisión duplex completa**

La transmisión duplex completa permite que los dos extremos transmitan y reciban simultáneamente, es una comunicación bidireccional y al mismo tiempo. Se tiene un canal físico y dos canales lógicos, como la conversación telefónica donde al no escuchar los dos extremos pueden hablar simultáneamente.

En la transmisión analógica full duplex se requiere utilizar dos frecuencias o dos cables si se quiere emitir y recibir en la misma frecuencia.

En la transmisión digital full duplex se requieren en medios guiados dos cables por conexión uno para un sentido y otro para el sentido contrario.

- **Transmisión en paralelo**

En este modo de transmisión los n bits que componen a cada byte o carácter se transmiten al mismo tiempo en grupo en un solo ciclo de n bits. Tiene las siguientes características:

- Este modo se utiliza mas comúnmente en los ordenadores para realizar la transferencia interna de los datos simultáneamente como un conjunto de bits que forman una palabra, esto se hace transmitiendo varias señales simultáneamente a través de 8 líneas de datos
- Se transmite cada conjunto de n bits, seguido por un espacio de tiempo y luego nuevamente otro conjunto de n bits y así sucesivamente.

- La transmisión en paralelo puede usar dos formas de transmisión distintas. Una dispone de n líneas diferentes a razón de una por bit a transmitir; la otra usa una sola línea pero enviando cada bit mediante el procedimiento llamado multiplexación.
- Este tipo de transmisión se emplea generalmente para altas velocidades ya que es su característica más importante, enviar mas bits en el menor tiempo posible, sus velocidades se miden en bytes o caracteres por segundo.
- Se usa para distancias cortas que no superan las decenas de metros (la distancia máxima es de 100 pies) pues el tiempo de llegada de los bits difiere de una línea a otra lo cual se acentúa mas con el aumento de la distancia, además de que se necesitarían tantas líneas de larga distancia como bits a transmitir lo cual no es muy costeable ni una buena solución, mas bien seria un desperdicio de recursos, ya que a mayor distancia no solo se encarecen los cables sino que también los transmisores y receptores son mas complejos debido a la difícil que es transmitir pulsos a través de cables largos.

- **Transmisión en serie**

Por lo costoso de la transmisión en paralelo se usa una sola línea para la transmisión en serie la cual envía los bits uno detrás del otro. Es más lenta que la transmisión en paralelo debido a su característica de secuenciamiento de bits ya que los bits que componen cada carácter se transmiten en n ciclos de 1 bit cada uno. Sus características son:
- El envío de los bits es uno detrás de otro hasta completar cada carácter.
- Es el sistema de transmisión típico de los sistemas teleinformáticos.
- En ocasiones realiza una deserialización y serialización ya que las señales que son transmitidas por los enlaces de telecomunicaciones al llegar a los equipos informáticos deben pasar al modo paralelo y viceversa.
- La secuencia de los bits se realiza en sentido contrario de cómo se escriben las cifras en el sistema de numeración binario. Cuando se transmite con bit de paridad este se transmite siempre en ultimo termino.
- Usada para transmitir a larga distancia.
- Se tiene una sola línea para transmitir los datos.

La transmisión en serie tiene dos procedimientos, la transmisión asíncrona y síncrona.
Sincronía
La sincronización es una de las mayores características de los sistemas de comunicación digitales, esta es empleada por los elementos en comunicación para tener un control de la transmisión. Cuando se establece una comunicación debe haber una sincronización entre el emisor y el receptor, esta sincronización de la transmisión debe implementarse debido a los problemas que se tienen para recuperar una señal transmitida, ya que se necesita saber cada cuanto tiempo va a llegar un dato o para que el receptor conozca el tamaño y duración de los paquetes, esto es el receptor necesita saber en que momento llega un bit 1 o 0. Esto es la sincronización, la sincronización es el proceso mediante el cual el emisor informa al dispositivo receptor sobre los instantes en que van a transmitirse las señales. De no hacerlo el receptor no tendrá el tiempo suficiente para ajustarse al flujo de datos perdiendo los primeros bits y por tanto parte de la información podría perderse irremediablemente.
Cuando se quiere establecer una comunicación debe haber una sincronización entre el emisor y el transmisor y así el receptor se enterara que se desea entablar comunicación con el, y conocerá cual es el tamaño y duración de los paquetes, para esto después de recibir la señal de sincronización deberán tener un reloj común sincronizado. Los sistemas de comunicación utilizan dos formatos de transmisión: la transmisión sincrona y la transmisión asíncrona.

- **Transmisión síncrona**

En la transmisión sincrona se usan canales separados de reloj que administran la recepción y transmisión de los datos. Al inicio de cada transmisión las siguientes señales preeliminares:

- Bytes de sincronización en los protocolos orientados a byte.
- Flags en los protocolos orientados a bit-

En el procedimiento de sincronía se tienen dos relojes, uno en el transmisor y otro en el receptor, este sistema de los dos relojes realiza una sincronización entre el emisor y receptor. La transmisión síncrona envía una trama de datos o conjunto de caracteres llamada información útil entre dos delimitadores, de los cuales los primeros son el conjunto de bits de sincronismo (SYN) y termina con otro conjunto de bits de final de bloque (ETB). Los bits de sincronismo tienen la función de alertar al receptor de la llegada de los datos y de sincronizar los relojes existentes en el emisor y el receptor, de tal forma que estos controlen la duración de cada bit y carácter. Las señales de reloj determinan la velocidad a la cual se transmite o recibe.

Este tipo de transmisión es muy eficiente para bloques grandes de datos, ya que como no usa bits de comienzo ni de parada se transmiten bloques de muchos bits. Este tipo de transmisión divide la información en bloques de 256 bytes y se agrega un campo de control en el que se introducen 3 caracteres de sincronismo en ASCII. Los bits de sincronismo y de datos forman un conjunto de bits que es llamado trama.

- **Transmisión asíncrona**

En este método de transmisión se acompaña a cada carácter de información con un bit de arranque (start) y uno o dos bits de parada (stop), estas señales se usan para:

- Avisar al receptor que llega un dato.
- Proporcionar suficiente tiempo al receptor para sincronizarse antes de que llegue el siguiente byte.

Por cada carácter que se envía se transmiten señales de arranque y paro en la siguiente forma:

Start(1 bit)+datos(8bits)+Paro(1 o 2 bits)

El bit de arranque tiene la función de sincronizar los relojes del transmisor y el receptor. El bit de parada se usa para separar un carácter del siguiente.

Para realizar esto se mantiene la línea a nivel 1 de tal forma que el primer 0 es el bit de arranque y enseguida se transmiten los bits correspondientes al carácter, terminando la transmisión con un bit 1, cuya duración mínima es entre una y dos veces la de un bit, la línea se mantiene en esta forma hasta el comienzo de la transmisión del siguiente carácter. Esta es la manera más fácil de realizar la sincronización, el problema es que cuando no se transmite ningún carácter la línea esta desocupada. Si el receptor es más lento o más rápido que el emisor se pueden producir errores como la delimitación de trama o cuando se introduce ruido durante la transmisión el receptor puede creer que se ha emitido un dato, para esto el método utiliza bits de paridad para detectar los errores. Este tipo de transmisión es sencillo y no es costoso aunque requiere muchos bits de comprobación y control.

Transmisión analógica y digital.
La transmisión de datos, dependiendo de la naturaleza de los datos y de las señales que se usan para trasmitir los datos, puede tener cuatro tipos de combinaciones de señales para realizar la transmisión de la información que generan una transmisión analógica o digital, estas combinaciones son:

Transmisión analógica
Una señal analógica es una señal continua que se propaga por ciertos medios.
Los datos analógicos se pueden representar por una señal electromagnética que posee el mismo espectro que los datos. La transmisión analógica usa señales analógicas para transmitir datos del tipo analógico o digital, por lo que podemos tener:

- Transmisión de datos analógicos mediante una señal analógica.
  Para realizar una transmisión de datos analógicos usando un canal analógico se tendrá que usar una señal analógica para transmitir la información, si coincide el ancho de banda de ambas señales se transmiten los datos tal cual, de otra manera se tiene que realizar una modulación analógica de los datos[1].

- Transmisión de datos digitales mediante una señal analógica.
  Para realizar la transmisión de datos digitales mediante señales analógicas (el canal es analógico), el transmisor tiene que modular la señal analógica para transmitir los datos digitales y se tiene que realizar la demodulación en el receptor para obtener los datos digitales de la señal analógica, se realiza un proceso de modulación digital[1].

El problema de la transmisión analógica es que la señal se debilita con la distancia por lo que se tiene que amplificar la señal cada cierta distancia.

Transmisión digital
Una señal digital es una serie de pulsos que se transmiten a través de un cable ya que son pulsos eléctricos.
Los datos digitales se pueden representar por una serie de pulsos de voltaje que representan los valores binarios de la señal.
La transmisión digital usa señales digitales para transmitir datos del tipo analógico o digital, por lo que podemos tener:

- Transmisión de datos analógicos mediante una señal digital.
  Para transmitir datos analógicos mediante una señal digital en un canal digital, en el transmisor se realiza una codificación de los datos analógicos para convertirlos a una forma digital y se decodifican en el receptor para obtener los datos analógicos. Se realiza una conversión de señal analógica a digital[2].

- Transmisión de datos digitales mediante una señal digital.
  La transmisión totalmente digital (los datos y el canal son digitales) envía los datos directamente por el medio si se dispone de dos niveles de tensión, si se tienen mas de dos niveles de tensión se convierten antes de ser enviados. Esto se conoce como codificación digital[3].

[1] Este tópico se tratara en el tema 1.9 Tipos de modulación
[2] La conversión analógica a digital se tratará en el tema 1.5 Conversión analógica a digital
[3] La codificación se vera en el tema 1.7 Codificación de la comunicación digital

La transmisión digital tiene el problema de que la señal se atenúa y distorsiona con la distancia, por lo que se tienen que introducir repetidores de señal cada cierta distancia.

La transmisión de la información en un sistema de comunicaciones es una de sus tareas principales ya que mediante una adecuada transmisión de información esta será entregada en el destino correcto, en el tiempo adecuado, con la rapidez y rendimiento suficiente para transportar la cantidad de información que se desee enviar puesto que la información tardía es inútil por ejemplo en una videoconferencia y con efectividad para asegurar que los datos se entregan en el destino correcto fiablemente sin que sean alterados durante la transmisión.

1.4 Sistemas de Comunicación Digital

Los sistemas de comunicación actuales son predominantemente digitales. Son digitales por que los datos de salida que se transmiten hacia el destino usan valores discretos. Para el caso de las telecomunicaciones digitales y el computo que son las áreas que han dado auge a los sistemas digitales los valores que manejan son los llamados bits o datos binarios, el cero (0) y el uno (1).
Los sistemas de comunicación son digitales por que usan la transmisión digital, esto es la transmisión de pulsos digitales entre dos puntos. La información de entrada puede ser digital o analógica, esta última primero se convierte en pulsos digitales antes de su transmisión y en el otro extremo se reconstruye su forma analógica.
Las señales digitales emplean dígitos para representar objetos del mundo real. En las computadoras se representa con dos estados: prendido-apagado o mediante el 1 y 0 del sistema binario de numeración.
Cualquier carácter o letra puede ser representado mediante un conjunto de 8 bits que se denomina un byte. Las transmisiones digitales tienen la ventaja de detectar y corregir los errores que se pudieran haber cometido durante el proceso de emisión-recepción.
Bit. Un bit es la unidad más pequeña de información y la unidad base en las comunicaciones digitales.
Byte. Un byte es el número de bits necesarios en un sistema de codificación para poder representar un carácter. Un byte puede tener un número variable de bits dependiendo de que se usen cinco, seis, siete u ocho bits para formar un carácter. Normalmente esta formado por 8 bits.
Palabra una palabra es un número de caracteres fijos (bytes) que por ejemplo un ordenador trata como una unidad, los caracteres pueden ser letras, números o símbolos especiales.
La evolución de los sistemas de comunicación analógicos a digitales fue un proceso en el que se fueron agregando poco a poco elementos al sistema que permitian realizar un manejo mas eficiente de la transmisión de la información.
En un sistema de comunicación digital para transmitir la información entre dos puntos, esta información se debe envasar en un contenedor para posteriormente enviarse a través de un canal. Si la información consiste en ideas, decisiones o estados de ánimo, la manera de enviarla a distancia es por medio de palabras, texto impreso, imágenes, ondas acústicas, ondas electromagnéticas o señales de humo, y los canales de comunicación para cada uno de ellos son el aire, el correo, un cable de televisión, el aire y la atmósfera. Estos medios imponen restricciones a los contenedores de información, un contenedor solo puede trasmitirse por su canal apropiado, actualmente se puede convertir un tipo de señal a otra para evitar estas restricciones.
Es indispensable adaptar los mensajes que contiene la información al canal por el que serán transmitidos. Esta función la realiza un codificador. El proceso de comunicación requiere que tanto el que origina el mensaje como el que lo recibe conozcan la forma en que fue codificada la información, que conozcan el código empleado. La necesidad de cubrir distancias cada vez mayores provoco que se utilizaran sistemas más complejos conforme lo permitían los avances científicos y tecnológicos, empezando a usar sistemas de codificación tan abstractos como la escritura misma. El sistema de comunicaciones que se muestra en la Fig. 1.4.1 contiene un codificador/decodificador.

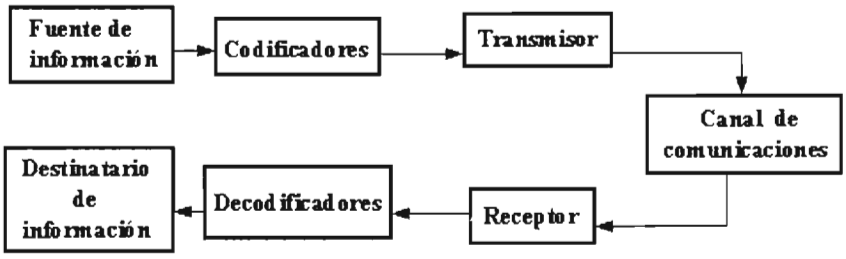


Fig.1.4.1 Sistema de comunicaciones con codificadores

Recordando brevemente cuales son los componentes[1] del sistema tenemos:

- Una fuente de información.
- Codificador. El codificador transforma los símbolos que emite la fuente en símbolos de un código (binario), mas adecuado para ser transmitido a través dc un canal de comunicaciones
- Transmisor de información cuya función es depositar la información de la fuente en un canal de comunicaciones
- Un canal de comunicaciones a través del cual se hace llegar la información de la fuente al destino
- Un receptor, extrae la información del canal y la entrega al destinatario
- Decodificador. Transforma los símbolos codificados a los símbolos originales que fueron emitidos por el emisor
- Un destinatario

Para hacer más eficiente la transmisión de la información se pensó en aprovechar mejor el ancho de banda del medio de transmisión para lo cual se empezó a realizar la compresión de la información como se muestra en la Fig. 1.4.2

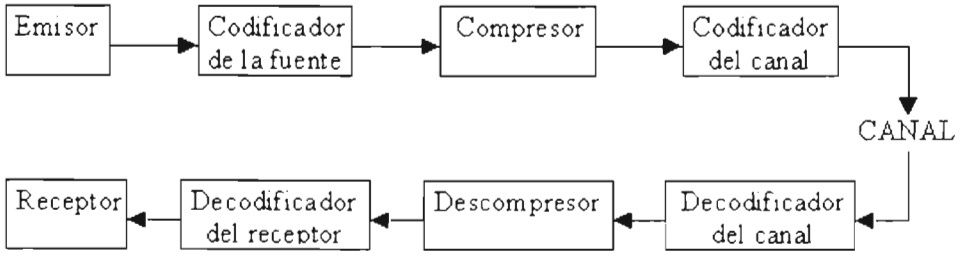


Fig. 1.4.2 Sistema de comunicaciones con compresores

Las funciones de los nuevos componentes son:

- Codificador de la fuente. Realiza el procesamiento necesario para convertir una señal analógica en una señal digital. Se compone de la conexión en serie de un muestreador, un cuantizador y un codificador.
- Compresor. Reduce el tamaño de la información para conseguir una transmisión más rápida
- Codificador de canal. Realiza una codificación adicional a la información orientada a que el receptor pueda detectar y corregir errores o alteraciones producidos en el canal debido a la presencia de ruido u otros factores.

[1] La función de estos componentes se describió en el tema 1.1

- Decodificador de canal. Decodifica el canal para detectar y corregir posibles errores que contienen los símbolos recibidos a través del canal.
- Descompresor. Descomprime los símbolos para regresarlos a su tamaño original si es que fueron comprimidos en la fuente.

Debido a estas implementaciones que se fueron agregando al tratamiento de la información es como llegamos a un esquema que representa en forma genérica un sistema de comunicaciones digitales como se muestra en la Fig. 1.4.3

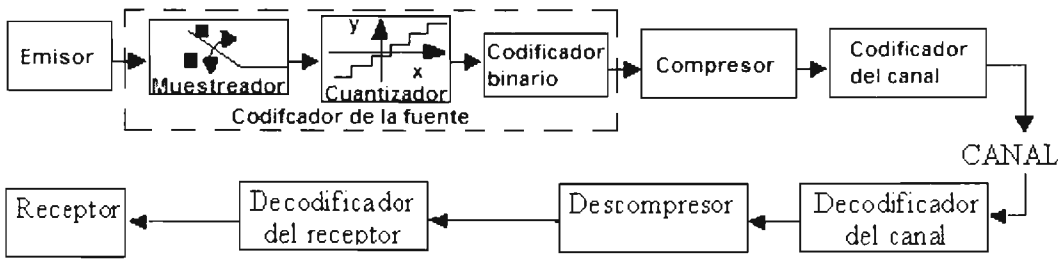


Fig. 1.4.3 Sistema de comunicaciones digitales

En la Fig. 1.4.3 no se muestran pero también se tienen componentes como:

- El modulador: el cual se ajusta generalmente a un oscilador para realizar alguna técnica de modulación
- El detector en el receptor para reproducir tan fielmente como sea posible la secuencia de señales de entrada
- El demodulador en el receptor que sirve para separar la modulación de la onda senoidal de alta frecuencia que introdujo en el transmisor

Los sistemas de comunicación digital desplazaron a las comunicaciones analógicas por muchas características y ventajas que los hacen más eficientes en la transmisión de la información, entre sus ventajas podemos mencionar las siguientes:

- La comunicación digital es más inmune al ruido de canal y a la distorsión de canal. Esto tiene su explicación en que en los sistemas analógicos se necesita evaluar con precisión los parámetros de amplitud, frecuencia y variaciones de fase y en la transmisión digital esto no se hace con mucha precisión ya que los pulsos se evalúan en un intervalo de muestreo y únicamente se determina si esta arriba o abajo o si es un 1 o un 0.
- Mayor exactitud para transmitir mensajes en presencia de señal y ruido
- Los repetidores regenerativos a lo largo de la trayectoria de transmisión detectan la señal y la retransmiten libre de ruido, esto no se puede hacer en la comunicación analógica en la cual se usan amplificadores que retransmiten y regeneran la señal junto con el ruido.
- La implementación del hardware digital es flexible, permitiendo usar circuitos integrados a gran escala LSI y a muy gran escala VLSI los cuales se han abaratado y además consumen menos potencia.
- Las señales digitales se pueden codificar para tener indices de error bajos, alta fidelidad y privacia mediante el cifrado, por lo que hay mas seguridad de la información.
- La utilización de banda ancha es mejor aprovechada por al tecnología digital.
- Las señales digitales se pueden multiplexar más fácilmente.

- La comunicación digital es más eficiente que la analógica para intercambiar la relación señal a ruido por ancho de banda.
- Uso del medio más eficiente. Esto es conseguido con las tecnologías de multiplexación en el tiempo (técnicas digitales) que son más baratas que la multiplexación en frecuencia (técnicas analógicas).
- Integración. Con el tratamiento digital de los datos analógicos y digitales todas las señales se pueden tratar de forma similar. Al tratar digitalmente todas las señales, se pueden integrar servicios de datos analógicos (voz, video, etc.) con servicios de datos digitales como texto.
- Almacenamiento y procesamiento. Las señales digitales se pueden guardar y procesar más fácilmente que las señales analógicas.
- Las señales digitales son más sencillas de medir y evaluar con esto se puede hacer una comparación más fácil de rendimiento entre sistemas digitales con diferentes capacidades de señalización e información
- Los sistemas digitales están mejor equipados para detectar y corregir errores

Pero también los sistemas digitales tienen algunas desventajas como son:

- Ancho de banda. La transmisión de las señales analógicas convertidas a digital ocupan más ancho de banda para transmitir que la señal analógica.
- Procesamiento adicional de señales cuando son analógicas para convertirlas a códigos digitales y nuevamente a analógicas en el receptor.
- Sincronización. La transmisión digital requiere de sincronización precisa de tiempo entre los relojes del transmisor y el receptor.
- Los sistemas de transmisión digitales son incompatibles con las instalaciones analógicas existentes.

Las tareas del sistema de comunicaciones son:

- Utilización del sistema de transmisión.
- Implementación de la interfaz.
- Generación de una señal.
- Realización de la sincronización.
- Gestionar el intercambio como la direccionalidad y el establecimiento de turnos.
- Controlar el flujo para que la fuente no sature al destino.
- Detectar y corregir errores.
- Direccionamiento y encaminamiento cuando se comparte el sistema de comunicación con dos dispositivos.

El desarrollo de los sistemas de comunicaciones y su evolución a los sistemas de telecomunicaciones provoco que las telecomunicaciones analógicas fueran desplazadas por las digitales, este mismo gran avance y el desarrollo de la informática han hecho que los sistemas de comunicación sean muy comúnmente vistos y analizados desde el punto de vista de comunicación de datos entre computadoras o sistemas de comunicación digitales como muestra la Fig. 1.4.4

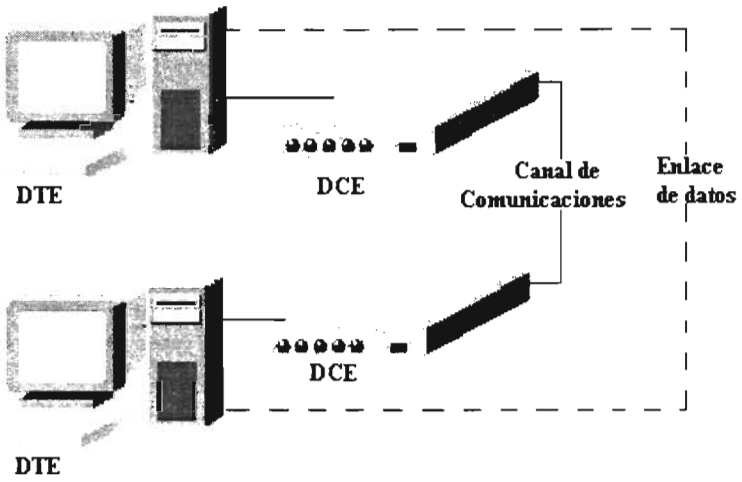


Fig. 1.4.4 Sistema de comunicaciones digitales

En un sistema de comunicación digital de datos entre computadoras los elementos que integran el sistema son:

- Equipos terminales de datos (DTE)

El DTE pueden ser la fuente o el destino de la información en este caso el equipo informatico, los equipos DTEs pueden ser desde terminales, ordenadores periféricos, microcomputadoras o hosts. El DTE tendrá un controlador de comunicaciones, que tiene las funciones de comunicación, incluyendo la detección y corrección de errores, elementos para controlar el dialogo y la interconexión de las interfaces con la red.

- Equipos terminales del circuito de datos (DCE)

Los Equipos DCE tienen la función de realizar la conversión entre el DTE y el canal de transmisión. Entre los equipos informaticos y las redes analógicas se conectan equipos que actúan como interfaz y son los equipos terminales de circuitos de datos (muy a menudo es el modem), los cuales se encargan de modular y demodular o multiplexar la señal, convierten las señales digitales generadas por los DTE en señales analógicas capaces de ser transmitidas por la red y viceversa, también realizan funciones como el establecimiento y liberación del circuito de comunicaciones.

- Línea de comunicaciones (LC)

Son los medios de trasmisión que permiten unir los dos equipos DCE o MODEM cuya constitución dependerá de la distancia, velocidad, etc. Y debe cumplir las especificaciones de la infraestructura de comunicaciones pública o privada.

- Enlace de datos (ED)

Es el circuito de unión entre los equipos DTE fuente y destino de los datos. Tanto al iniciarse el circuito como al finalizar las señales que salen o llegan del DTE de este circuito son señales digitales que entienden los equipos informaticos.

- Circuito de datos (CD)

Es el camino formado por los DCE y la línea de comunicaciones. Su misión es entregar en la interfaz con el DTE destino las señales bajo la misma forma e idéntica información que recibió en la interfaz con el DTE fuente.

Los sistemas de comunicación han tenido un gran desarrollo ya que basados en las tecnologías modernas cubren una amplia gama de servicios y aplicaciones que van desde la telefonía hasta la transmisión de datos por medio de redes donde las computadoras establecen diálogos, pasando por todos los sistemas de comunicación tan complejos de hoy día sin percatarnos de las diferentes modalidades, desde la radiodifusión hasta variantes de la telefonía celular.

La complementación mutua de diferentes tecnologías y el desarrollo paralelo y concurrente de muchas de ellas han dado lugar a los sistemas de telecomunicaciones con un grado de avance enorme. Se cuenta en estos días con una infraestructura de telecomunicaciones con cobertura global que ofrece una enorme variedad de sistemas interconectados proporcionando a los usuarios una gran diversidad de servicios de telecomunicaciones.

Servicios que van desde el servicio básico de telefonía con todas sus modalidades y versiones, local y larga distancia, IP, pasando por los distintos esquemas de radiotelefonía como la móvil y portátil, hasta llegar al videotexto, las redes privadas y publicas de transmisión de datos, así como las redes digitales con servicios integrados, la radiodifusión, la televisión con sus versiones vía cable y de alta resolución, servicios de valor agregado como el teletexto, el fax, la radio determinación, la localización de personas, de vehículos y de flotilla de vehículos en movimiento y casi todos los servicios que se prestan con las redes modernas (todos los que empiezan con tele: telemedicina, telebancos, telecompras, televotaciones, teleconferencias, etc.)

Con la comunicación de datos digitales se busca hacer un uso eficiente de la capacidad de un canal de comunicación consiguiendo la mayor velocidad de transmisión sin superar las tasas de error permitidas, teniendo en cuenta el ruido que se va a introducir.

1.5 Conversión de la comunicación analógica a digital

Con el surgimiento de los enlaces digitales para comunicar diferentes puntos surgieron las comunicaciones digitales. En las comunicaciones digitales se tiene el objetivo de transmitir la información al receptor por enlaces más limpios y libres de errores, los enlaces digitales.
Por el gran desarrollo y ventajas de los sistemas digitales seria ideal que el mundo de las telecomunicaciones fuera totalmente digital, desde los equipos hasta las señales que se manejan, para poder aprovechar el gran número de características y ventajas que presenta un sistema digital.
Sin embargo no se puede dejar de tratar a las comunicaciones analógicas ya que muchas de las señales en la vida real son de naturaleza analógica.
Para poder transmitir señales analógicas por canales digitales se debe realizar un proceso de digitalización o conversión analógica a digital A/D como muestra la Fig. 1.5.1, este proceso se realiza para adecuar la señal al canal de comunicación además de darle un mejor tratamiento y así tener un sistema más eficiente.

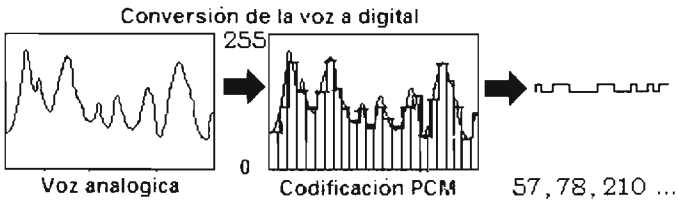


Fig. 1.5.1 Conversión de la voz analógica a digital

Por ejemplo si se quiere transmitir voz humana por un enlace digital como muestra la Fig. 1.5.1, la voz es una señal continua que tiene un rango de 0 a 4 Khz., tenemos en esta señal toda una serie de valores continuos infinitos mientras que las comunicaciones digitales se basan en el manejo de señales discretas. Por esta diferencia de la naturaleza de señales se tiene que realizar una conversión de la señal analógica a digital.
Recordemos que un sistema analógico en las telecomunicaciones y el cómputo significa todo aquel proceso de entrada/salida cuyos valores son continuos. Continuo es todo aquello que puede tomar una infinidad de valores dentro de un cierto limite, superior e inferior.
Un sistema digital involucra valores de entrada/salida discretos. Discreto es algo que puede tomar valores fijos. En el caso de las comunicaciones digitales y el cómputo, esos valores son los Bits (BInary DigiTs), el cero (0) y el uno (1).

Proceso de la conversión analógica a digital
El proceso de conversión analógico a digital (A/D) se hace básicamente en tres etapas Fig.1.5.2:
- Muestreo.
- Cuantificación.
- Codificación.

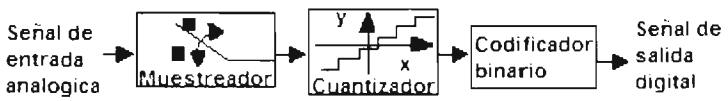


Fig. 1.5.2 Etapas de la conversión analógica a digital

Muestreo

La conversión analógica a digital es realizada tomando muestras de la señal analógica y representando el nivel de la señal con un numero que es transmitido sobre el enlace digital. El muestreo se realiza de acuerdo con el teorema de Nyquist.

Teorema de muestreo de Nyquist:

No se necesita observar todo el tiempo una señal analógica o continua en tiempo para poder decir cual es su valor en cualquier momento, aunque la señal no haya sido observada en ese instante. Es suficiente observar sus valores o muestras en instantes iguales y suficientemente cercanos entre sí para reconstruir la señal de la misma forma que si no se hubiera dejado de observar la señal en ningún instante. El tiempo entre las observaciones o muestras debe ser lo suficientemente pequeño para poder captar aun las variaciones más rápidas. La razón de muestreo debe ser igual, o mayor, al doble del ancho de banda de la señal analógica.

Es decir que el numero mínimo de muestras de una señal que se requieren para reconstruir dicha señal es igual a dos veces la máxima frecuencia de la señal.

Por ejemplo si se va a hacer un muestreo de la señal de voz cuyo rango de frecuencias es 0-4 Khz. por el teorema de Nyquist tendríamos que tomar 2*4k=8k muestras por segundo

De esta manera en lugar de tener que guardar toda la evolución de una señal a lo largo del tiempo, es suficiente guardar un conjunto de las muestras de la señal sin perder la posibilidad de reconstruir toda la señal a partir de sus muestras

Para comprender un poco mas el teorema de Nyquist, obsérvese el circuito de la Fig. 1.5.3 que realiza el muestreo a 8Khz

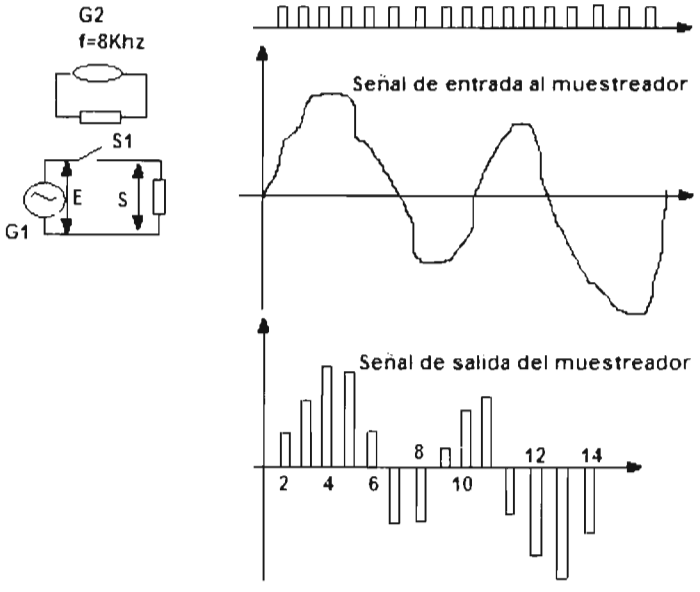


Fig. 1.5.3 Circuito muestreador

El generador G1 produce una señal E a 1 Khz., el interruptor S1 es controlado para abrir y cerrar mediante el generador de pulsos G2 a una velocidad de 8 Khz., el tiempo que permanece cerrado el interruptor son 1/8000= 125 mseg. Entonces la señal E es modulada por el interruptor y el voltaje S son los pulsos con amplitud igual al de la señal analógica E en los instantes mostrados, esta amplitud cambia durante el intervalo

de muestreo pero si los intervalos son muy pequeños este cambio no es muy significativo. El análisis espectral de la señal muestreada de la Fig. 1.5.4(a) nos muestra que el espectro de la señal original aparece reproducido con ambas bandas centradas en frecuencias múltiplos de la frecuencia de muestreo f=8 Khz., en la Fig. 1.5.4(b) se muestra el mismo espectro pero con una frecuencia de muestreo que no cumple el teorema de Nyquist, lo que provoca un traslape de los espectros adyacentes que hacen se pierda información de la señal original.

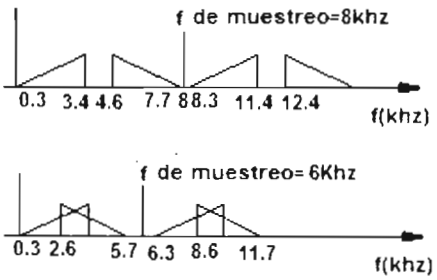


Fig. 1.5.4 Espectro de la señal muestreada

El muestreador tiene como entrada una señal continua en el tiempo y a su salida una señal discreta en el tiempo, esta etapa de la conversión A/D funciona como un interruptor que abre y cierra para poder tomar muestras de la señal en diferentes instantes de tiempo, cada muestra tomada tendrá una amplitud igual o proporcional a la de la señal original en el tiempo de muestreo, Fig. 1.5.5

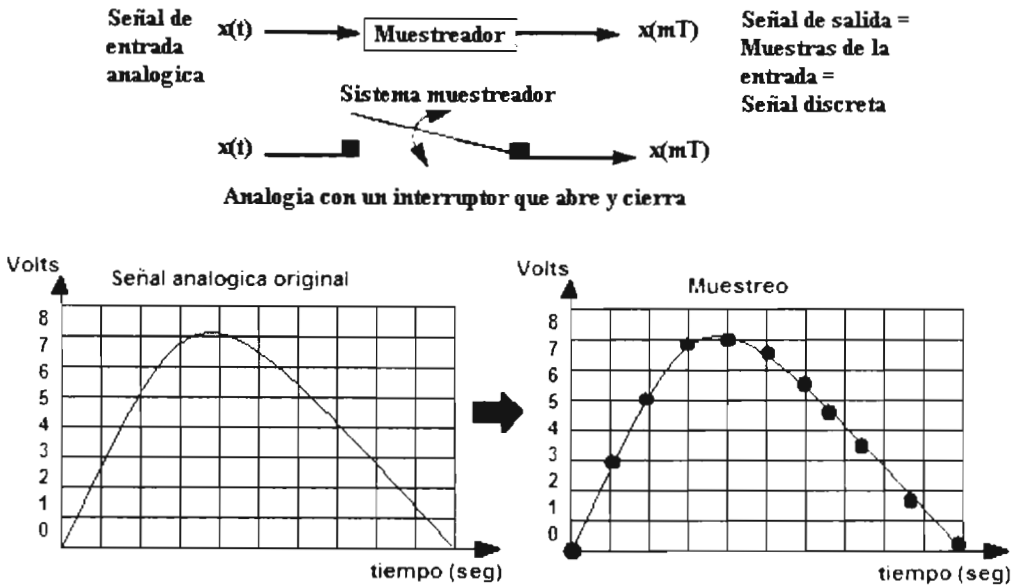


Fig. 1.5.5 Sistema de muestreo

Los valores de la muestra se usan para modificar ciertos parámetros de un tren de pulsos periódicos, se puede modificar la amplitud, anchura o posición de los pulsos en proporción a los valores de las muestras con lo que podemos tener una modulación por amplitud de pulsos (PAM), modulación por anchura de pulsos (PWM) o modulación por posición de pulsos (PPM), la Fig. 1.5.6 muestra la señal analógica y las correspondientes formas de pulsos moduladas.

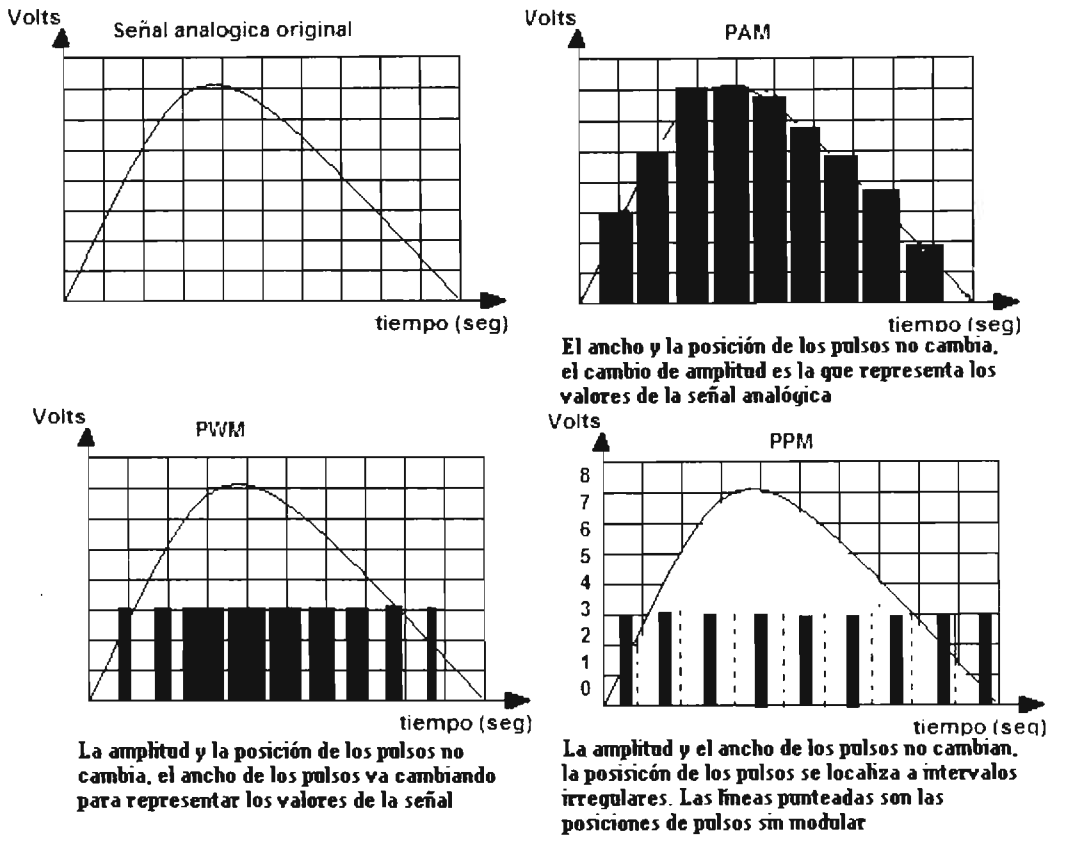


Fig.1.5.6 Señales moduladas en pulso PAM, PWM, PPM

Para una señal de ancho de banda limitado la frecuencia de muestreo es:

$$f_m > 2 \cdot B$$

Donde:

- f_m es la frecuencia de muestreo medida en Hertz (hz.). Esta frecuencia se conoce como razón de muestreo de Nyquist.

- B es el ancho de banda de la señal.

La frecuencia de muestreo en un segundo se conoce como la razón de muestreo en Hz. Esta razón de muestreo determina el rango de frecuencias (ancho de banda) de un sistema de comunicaciones.
A mayores frecuencias de muestreo habrá mas calidad o precisión pero se pierde en ancho de banda, es decir entre mas muestras se tomen de una señal más cercana a la original será la señal digitalizada y será de mas calidad aunque el ancho de banda ocupado será mayor.
El muestreo se realiza en el dominio del tiempo por que es el tiempo de captura de una señal.
Los valores obtenidos de las muestras no son todavía digitales ya que se encuentran dentro de un rango continuo y pueden tomar cualquier valor de un rango infinito de valores por lo que se debe proceder a realizar la cuantificación.

Cuantificación

- El proceso de cuantización convierte valores continuos en valores discretos, esto se hace aproximando cada muestra al nivel cuantificado más próximo. Mientras el muestreo es el tiempo de captura de una señal, la cuantización es el componente en amplitud del muestreo. Dependiendo del numero de bits usados será el numero de niveles usados para la cuantificación.

La entrada al cuantizador es una señal continua y la salida es una versión cuantizada, si la entrada es continua en el tiempo y amplitud la salida es continua en el tiempo pero discreta en amplitud, Fig. 1.5.7

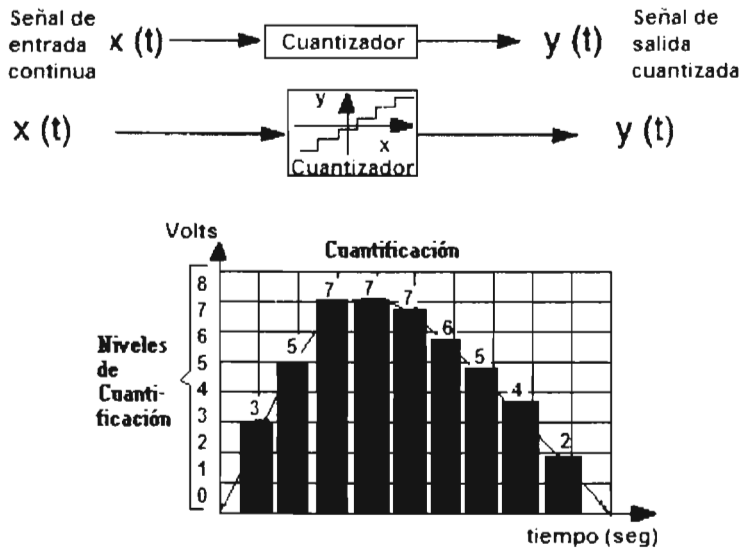


Fig. 1.5.7 Sistema de cuantificación

La cuantificación se hace en el dominio de la amplitud ya que la amplitud de una señal analógica es representada en una serie de pasos discretos, estos pasos o intervalos de cuantificación se conocen como los pasos de cuantificación. Cada paso esta dado en un numero binario que digitalmente codifica el nivel de la señal.

Entre mayor sea el numero de niveles para cuantificar nos dará una mejor reconstrucción de la señal. El numero de niveles de cuantificación es determinado por el numero de bits que forman la palabra digital con la que se representa cada valor de amplitud.

Por lo tanto se debe tomar el mayor numero de muestras en tiempos menores y se deben cuantizar a mayores niveles o con mas bits ya que si no se hace esto, se pueden generar errores de cuantificación (ruido de cuantificación), los cuales provocan que la reconstrucción de la señal original sea muy cuadrada.

Error de cuantificación

Es la diferencia entre el valor original de la amplitud muestreada y el valor aproximado correspondiente a la escala seleccionada, la magnitud del error es determinado por la fineza de la escala usada, este error es provocado por la asignación al conjunto de valores que se encuentran entre un intervalo de muestreo el mismo valor digital.

En el proceso de cuantificación es muy importante que el error de cuantificación sea lo mas bajo posible, para disminuir la relación entre el error de cuantificación y la señal de entrada se usan diferentes técnicas de cuantificación:

- Cuantificación lineal
- Cuantificación logarítmica

- Cuantificación no lineal
- Cuantificación vectorial

- Cuantificación lineal (uniforme):
  En la cuantificación lineal la relación entre la señal de entrada y la señal de salida es lineal, Fig. 1.5.8, en esta técnica de cuantificación se tiene un rango de valores distribuidos uniformemente para decidir cual es el valor de la señal, por lo que la distancia entre los niveles de reconstrucción es siempre la misma, esto es, los pasos de cuantificación son todos del mismo tamaño. El problema de la cuantificación uniforme es que conforme aumenta la amplitud de la señal también aumenta el error de cuantificación.

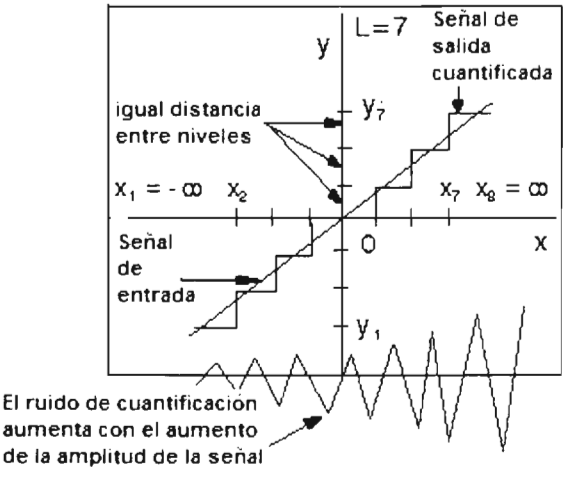


Fig. 1.5.8 Cuantificación lineal

Los cuantificadores lineales no hacen ninguna suposición de la naturaleza de la señal a cuantificar de ahí que no proporcionen los mejores resultados, sin embargo son sencillos y de bajo costo de implementación.

- Cuantificación logarítmica:
  Las señales de voz pueden tener un rango dinámico superior a 60 dB. Para conseguir una alta calidad de voz se deben usar un elevado numero de niveles de reconstrucción. Es muy importante que la resolución del cuantificador sea mayor en las partes de la señal de menor amplitud que en las de mayor amplitud. En la cuantificación lineal se desperdician niveles de reconstrucción y por lo tanto ancho de banda. Esto se puede mejorar incrementando la distancia entre los niveles de reconstrucción conforme aumenta la amplitud de la señal.

Para implementar la mejora se hace pasar la señal por un compresor logarítmico antes de la cuantificación. Esta señal comprimida se cuantifica uniformemente o linealmente. A la salida del sistema la señal pasa por un expansor, que realiza la función inversa al compresor. Esta técnica es conocida como compansión. Para realizar la compresión se usan dos funciones que se conocen como Ley-A (usada en Europa y Latinoamérica) y la Ley-μ (usada en EU):

$$c(x) = \begin{cases} \dfrac{A|x|}{1 + \log_e A}\,\mathrm{sgn}(x) & \text{si } 0 \le \dfrac{|x|}{x_{max}} \le \dfrac{1}{A} \\ x_{max}\,\dfrac{1 + \log_e (A|x| / x_{max})}{1 + \log_e A}\,\mathrm{sgn}(x) & \text{si } \dfrac{1}{A} \le \dfrac{|x|}{x_{max}} \le 1 \end{cases}$$

Ley-μ

$$c(x) = x_{max}\,\frac{\log_e (1 + \mu |x| / x_{max})}{\log_e (1 + \mu)}\,\mathrm{sgn}(x)$$

En la mayoría de los sistemas telefónicos A=87.56 y μ=255. La Fig.1.5.9 es la grafica de la ley-μ para distintos valores de μ

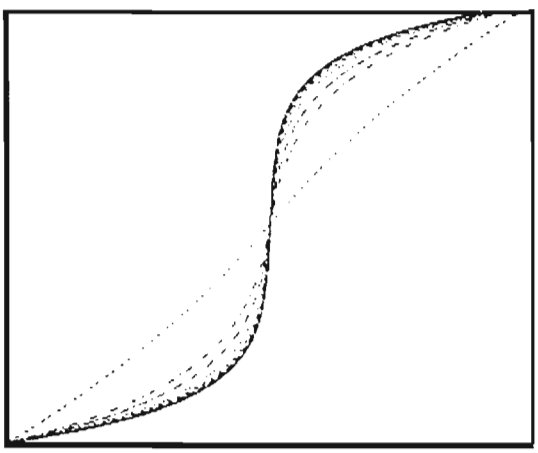


Fig. 1.5.9 Distintos valores de la Ley-μ

- Cuantificación no lineal:
  En este tipo de cuantificación la relación entre la señal de entrada y la señal de salida no es lineal, ya que agrupa los intervalos de cuantificación a lo largo del eje de forma no uniforme, como se muestra en la Fig. 1.5.10.

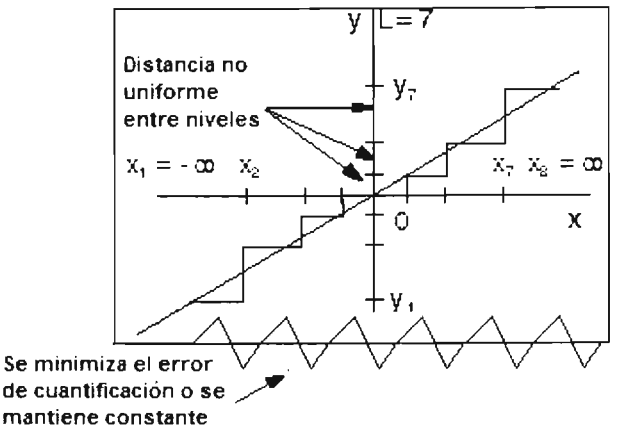


Fig. 1.5.10 Cuantificación no lineal

Este tipo de cuantificación es usado cuando la distribución probabilística de una señal no es uniforme, sino que tiene preferencia por una cierta zona de voltaje como las señales de voz, entonces el cuantizador no uniforme establece pasos más estrechos en las zonas de voltaje mas frecuentes y pasos mas grandes en zonas menos probables. Así en la Fig. 1.5.10 la señal tiene preferencia de ocurrencia en voltajes alrededor del cero.
Si se conoce la función de la distribución de probabilidad, se pueden ajustar los niveles de reconstrucción a la distribución de forma que se minimice el error cuadrático medio. Esto significa que la mayoría de los niveles de reconstrucción se den en la vecindad de las entradas más frecuentes y por lo tanto se minimice el error de cuantificación debido a que da mas resolución a las muestras de valor más pequeño y menos resolución a las muestras de mayor valor.
La curva de la Fig. 1.5.11 representa la cuantificación no uniforme, en la cual podemos ver que expande los valores de bajo voltaje y comprime los de alto voltaje, realizando el proceso de compansión (compresión y expansión)

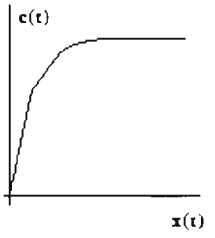


Fig. 1.5.11 Curva de la cuantificación no uniforme.

Se puede usar una estimación de la distribución para diseñar los cuantificadores, la cual se obtiene a partir de los datos a cuantificar de forma iterativa.

- Cuantificación vectorial
  En los métodos de cuantificación lineal, no lineal y logarítmica cada muestra se cuantifica independientemente de las muestras vecinas. Esta no es la mejor forma de cuantificar los datos de entrada. Es más eficiente cuantificar los datos en bloques de N muestras. El bloque de N muestras se trata como un vector N-dimensional. La Fig. 1.5.12 muestra un ejemplo de cuantificación vectorial (VQ) en dos dimensiones.

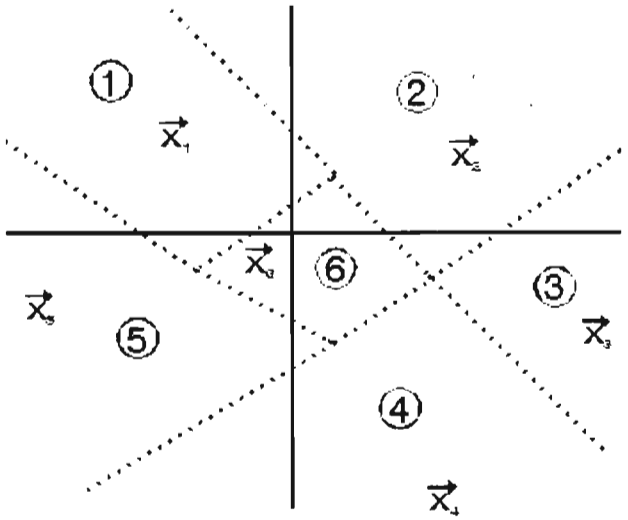


Fig. 1.5.12 Cuantificación vectorial

De la Fig. 1.5.12 se observa al plano XY dividido en seis regiones distintas. El vector de entrada con dos componentes se reemplaza por el centroide i (que representa todos los vectores de una determinada región i) de la región a la que pertenece.. Este tipo de cuantificación proporciona mejores resultados que la cuantificación escalar, pero es más sensible a los errores de transmisión y lleva consigo una mayor complejidad computacional.

Codificación

Del proceso de cuantificación la señal queda ahora si digitalizada, por lo que se procede a su codificación para representar las muestras cuantificadas mediante algún código.

La codificación es la representación en pulsos digitales de las muestras cuantificadas usando códigos ya establecidos y estándares, el código mas utilizado es el código binario, existen otros códigos empleados.

Sobre la base del numero de bits que compongan al código será el numero de niveles que tendremos para cuantificar la señal. La codificación se muestra en la Fig. 1.5.13.

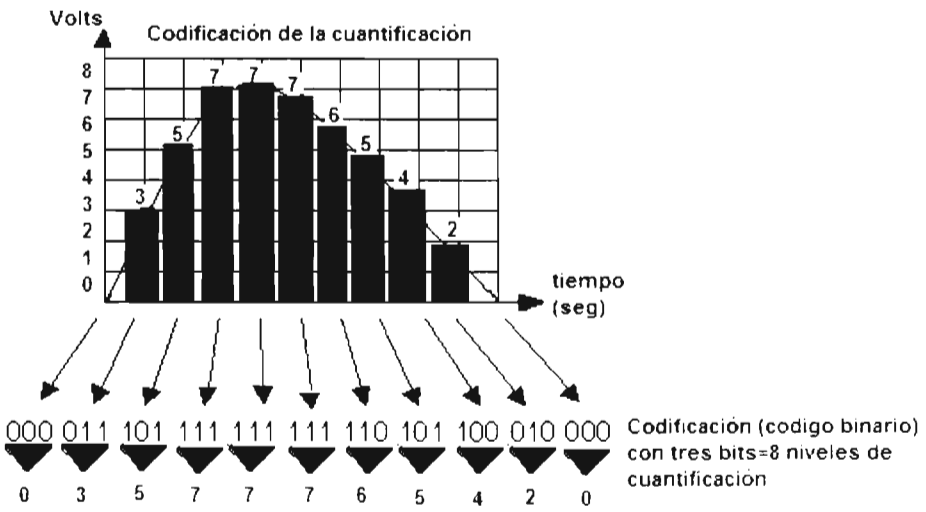


Fig. 1.5.13 Codificación de la señal muestreada

De esta forma queda digitalizada la señal analógica de entrada, únicamente resta convertir los códigos digitales a pulsos binarios.

PCM

Uno de los métodos mas utilizados para la codificación digital es el sistema PCM.
La modulación por código de pulsos (PCM) es un proceso digital de modulación para convertir una señal analógica en un código digital. En el proceso PCM de la señal analógica se toman muestras periódicamente, después en un convertidor analógico/digital los valores se cuantifican, se convierten en un numero binario y se codifican en un tren de impulsos. El tren de impulsos es una señal de alta frecuencia portadora de la señal analógica original.
El proceso PCM se basa en el teorema de muestreo de Nyquist, por lo que toma $2f_{max}$ muestras de la señal analógica, este proceso tiene tres etapas:

- Modulación por amplitud de pulsos (PAM)
- Modulación PCM
- Tasa de prueba

PAM

El primer paso en la conversión analógica a digital es la modulación por amplitud de pulsos PAM (recordemos que también podemos hacer una modulación por anchura de pulsos PWM o modulación por posición de pulsos PPM), esta recoge información analógica, hace un muestreo y genera pulsos basados en la prueba, la prueba se refiere a la medida de la amplitud a intervalos iguales, como se observa en la Fig. 1.5.14

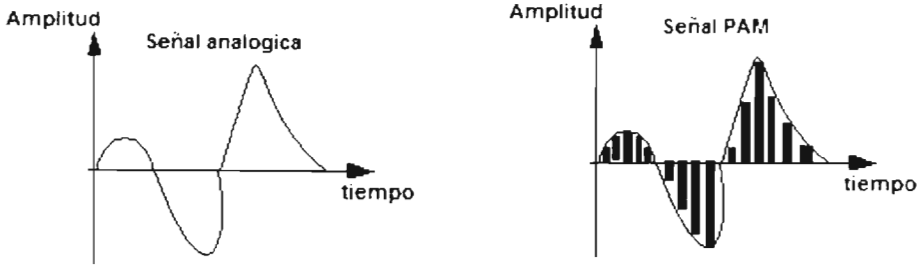


Fig. 1.5.14 Modulación por amplitud de pulsos

PAM convierte la señal analógica a pulsos, pero estos pulsos siguen teniendo amplitud, por lo tanto siguen siendo una señal analógica, para hacerlos digitales se hace uso de PCM.

Modulación PCM

PCM modifica los pulsos creados por PAM para hacer una señal completamente digital, primero cuantifica los pulsos para darles valores. La cuantificación se muestra en la Fig. 1.5.15

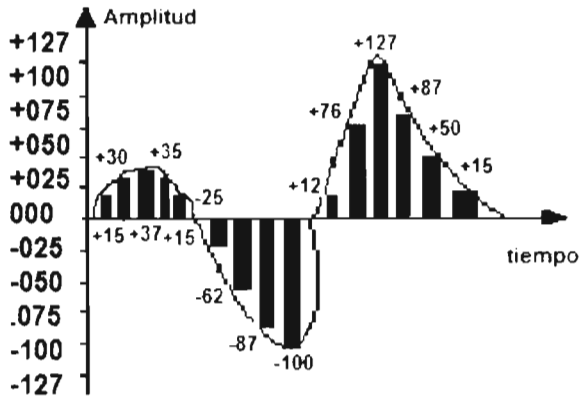


Fig. 1.5.15 Señal PAM cuantificada

En la Fig. 1.5.15 se asigna un signo y valor a las muestras, cada valor es traducido en su equivalente binario, con el octavo bit usado como signo, si el valor de la muestra es positivo se pone el octavo bit a 0 y si es negativo se pone un 1. Los equivalentes binarios de las muestras son:

+15=00001111 -25=10011001 +12=00001100
+30=00011110 -62=10111110 +76=01001100
+37=00100101 -87=11010111 +127=01111111
+35=00100011 -100=11100100 +87=01010111
+15=00001111 +50=00110010
+15=00001111

Finalmente los dígitos binarios son transformados en una señal digital de pulsos como muestra la Fig. 1.5.16

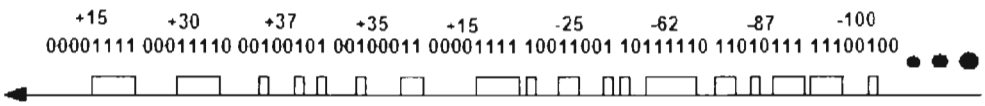


Fig. 1.5.16 Tren de pulsos digitales generados con PCM.

El proceso PCM completo se observa en la Fig. 1.5.17

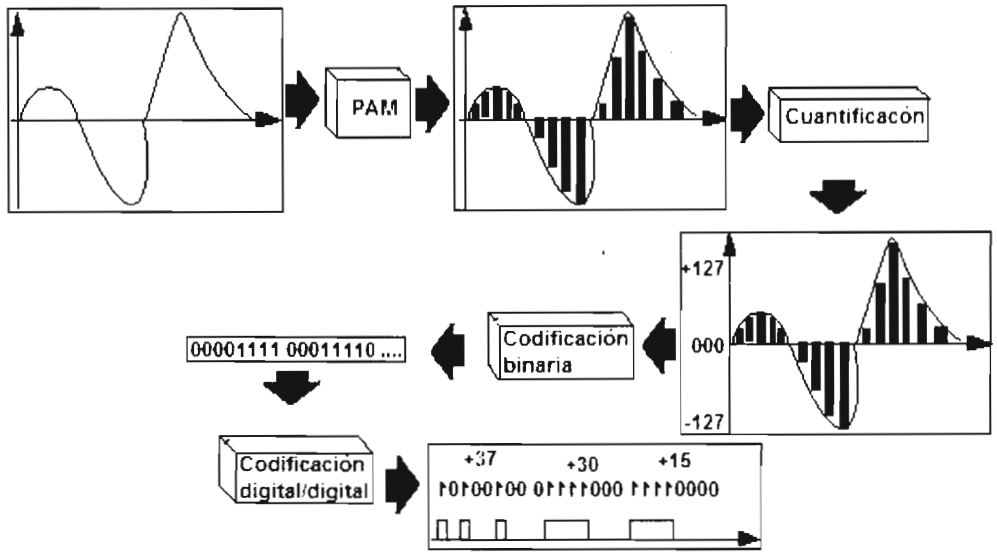


Fig. 1.5.17 Conversión de señal analógica a código digital PCM

Leyes de codificación para PCM

En PCM se tienen dos leyes de codificación no uniforme: la ley μ (usada en EU y Japón) y la ley A (usada en Europa y Sudamérica). Ambas usan un numero de bits de 8, lo que determina una frecuencia de muestreo de 8 Khz. y una velocidad binaria de 64 kbps. Las dos leyes producen una compresión de la curva de transferencia entre el nivel de la muestra S y la salida cuantificada Q, el calculo de estas se realiza con las siguientes formulas:

Ley μ $Q=\ln(1+\mu*S)/\ln(1+\mu)$ para $0\leq S\leq 1$ y $\mu=255$

Ley A $Q=(A*S)/(1+\ln \mu)$ para $0\leq S\leq 1/A$ y $A=87.6$

$Q=[1+\ln (A*S)]/(1+\ln A)$ para $1/A\leq S\leq 1$ y $A=87.6$

Estos valores teóricos son aproximados por 8 segmentos para la ley μ y 7 segmentos para la ley A (los dos primeros segmentos son colineales), el primer segmento es común para señales positivas y negativas en la Fig. 1.5.18 se muestra una aproximación para la ley A.

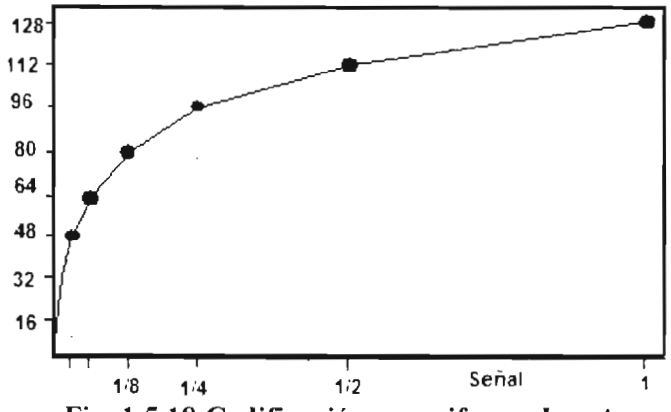


Fig. 1.5.18 Codificación no uniforme Ley A

Cada codificación en 8 bits responde a la secuencia binaria PSSS NNNN. Donde el primer digito indica la polaridad (P=1 para niveles positivos y P=0 para niveles

negativos), 3 bits de segmento para codificar las 8 divisiones(000 corresponde al primer segmento y 111 al segmento superior) y 4 bits para codificar los 16 niveles dentro de cada segmento.
PCM es el método usado para digitalizar la voz el cual divide el nivel en 256 niveles mediante el uso de 8 bits para representar cada uno de los niveles, de aquí se deriva el ancho de banda necesario de los enlaces de 64 kbits por segundo ya que si se digitaliza la voz que tiene una frecuencia máxima de 4 Khz., se tendrán que tomar muestras cada 2*4Khz=8 Khz. y como se usan 8 bits para representar cada muestra se necesitaría un ancho de banda de 8*8Khz=64 kbits por segundo para transmitir la señal de voz por un canal digital.

Transmisión por división de tiempo

Una señal por pulsos ocupa solo una parte del canal de comunicación, por lo que se pueden intercalar varias señales en el mismo canal.
La modulación por pulsos permite la transmisión simultanea de varias señales de banda base sobre una base de tiempo compartido lo que se conoce como multiplexión por división de tiempo (TDM).

Multiplexación
Cuando las necesidades de comunicación se incrementan se puede transferir mas de un solo canal entre dos sitios. La multiplexación es una forma de mandar algunos o muchos canales sobre una sola línea, se usa para transmitir varias fuentes de información como voz, datos o video sobre un mismo canal de comunicación, previamente digitalizados.
La Multiplexación por División de Tiempo (TDM) es la técnica de multiplexación mas usada actualmente aunque también se cuenta con la Multiplexación por División de frecuencia (FDM) y la Multiplexación por División de Longitud de onda (WDM).
La técnica de multiplexar parte del hecho de que si tenemos un canal para transmisión de 64 kbps, un bit se transmitirá cada 1/64000 seg. =15.6 μseg. de aquí surge la idea de realizar la transmisión a diferentes tiempos por ejemplo la mitad del tiempo.

Funcionamiento de TDM

Suponiendo que se tienen 3 canales cada uno transmitiendo cada 3 seg. Como muestra la Fig. 1.5.19

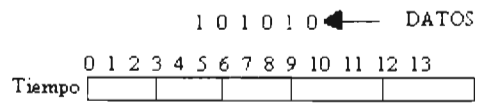


Fig. 1.5.19 Canal transmitiendo un bit cada 3 seg.

Como se puede ver podemos aprovechar el tiempo entre cada transmisión de bits para intercalar más información como muestra la Fig. 1.5.20.

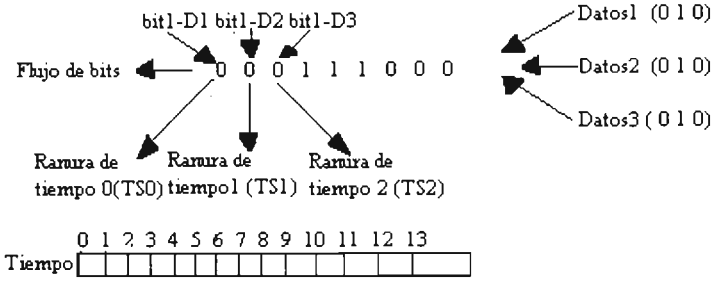


Fig. 1.5.20 Multiplexación a 3 canales

De la misma forma si tenemos 32 canales, cada uno a una velocidad de 64 kbps. Un multiplexador toma el primer byte de cada uno de los 32 canales y los manda uno después de otro. Después toma el siguiente byte de cada canal y así sucesivamente.
El multiplexador debe ser capaz de mandar todos los 32*8 bits de los 32 canales sin que el segundo byte del primer canal se pierda. La velocidad del multiplexador debe ser de 32*64Kbps o 2048 kbps.
Se llama TDM por que al multiplexor le toma 1/(8000*32) segundos mandar cada byte.
En la Fig. 1.5.21 Tenemos un ejemplo de un TDM de 3 canales

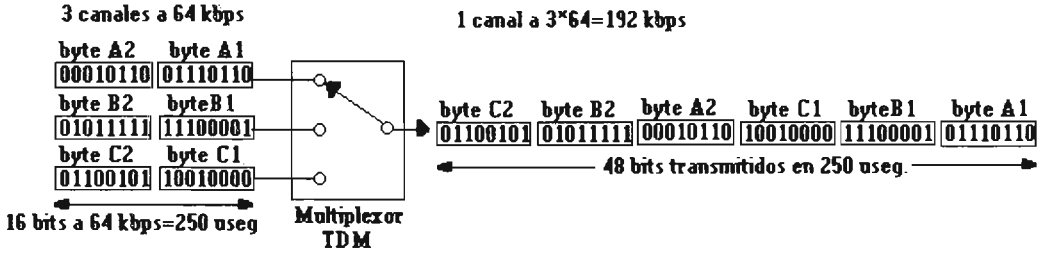


Fig. 1.5.21 Multiplexación de 3 canales de 64 kbps cada uno.

En el flujo de bits se mandan algunos bits especiales usados para la sincronización. Estos bits le indican a la punta receptora o sea el demultiplexor donde un nuevo grupo de 32 bytes empieza, y para que sepa como dividir los siguientes bits entre los canales. La sincronización no es necesaria para distinguir entre cada uno de los 32 canales.
Los equipos que usan la técnica TDM pueden usar una de dos tecnologías estándares existentes, el E1 que principalmente es usado en Europa y el T1 principalmente usado en Norteamérica. Ambos estándares empiezan con un solo canal de 64kbps, y pueden incrementar el numero de canales hasta llegar a 32 canales para el E1 y 30 para el T1, a partir de un E1 o T1 el incremento sucesivo de canales se realiza sucesivamente en múltiplos de los 32 o 30 canales para formar jerarquías. Cada incremento es acompañado por un incremento en la velocidad de bits de la línea.
El desarrollo de los sistemas de transmisión digital creció mucho en los 70's con el método de modulación PCM, en los 80's se hicieron más complejos para poder satisfacer las demandas de trafico, pero el alto costo de los equipos digitales era una limitante, por lo que se creo una técnica de modulación que combinaba tasas graduales no sincronas a la que se llamo pleosiocrona derivando en el termino PDH (Plesiochronous Digital Hierarchy) conocido actualmente.
Este desarrollo de los sistemas de transporte condujo a las dos principales infraestructuras de hoy en día que son PDH y SDH/SONET(Synchronous Digital Hierarchy/Synchronous Optical Network).

Infraestructura PDH

La infraestructura PDH esta basada en líneas de cobre por lo que define sistemas de transmisión que utilizan dos pares de alambre uno para la transmisión y el otro para la recepción y el método de multicanalización por TDM para intercalar canales de voz y datos digitales. Plesiocrono proviene de griego plesio (que significa cercano o casi) y cronos (reloj), lo que significa que dos relojes están cercanos uno del otro en el tiempo, pero no son exactamente los mismos, esta es su diferencia con isócronos que significa mismo reloj. Esta infraestructura es conocida ampliamente por los estándares de transmisión E1 y T1.

Sistema PDH Europeo

El E1 que define el estándar PDH Europeo definido por la ITU, es utilizado por el resto del mundo incluyendo México. Consiste de 30 canales de 64 kbps (canales E0) y 2 canales reservados para señalización y sincronía, dando una capacidad total de 2.048 Mbps. Existen E1s fraccionales. Las Jerarquías de transmisión por líneas de cobre para la norma Europea PDH se muestran en la tabla 1.5.1

Nombre Jerarquia PDH Europea (transmisión eléctrica)	Velocidad en bits	Canales	Capacidad
E0	64 kbps	1	1 canal
E1	2.048 Mbps	30	30 canales
E2	8.448 Mbps	120	4xE1
E3	34.368 Mbps	480	4xE3
E4	139.264 Mbps	1920	4xE4
E5	565.48 Mbps	7680	4xE4

Tabla 1.5.1 Jerarquías de transmisión PDH para la norma europea E1.

Sistema PDH Americano

El T1 que define el estándar PDH de Norteamérica consistente de 24 canales de 64 kbps (canales DS0) dando una capacidad total de 1.544 Mbps. Existen T1s fraccionales. Las jerarquías de transmisión por líneas de cobre para la norma Americana PDH se presentan en la tabla 1.5.2.

Nombre Jerarquía PDH Americana (transmisión eléctrica)	Velocidad de bits	Canales	Capacidad
DS0	64 kbps	1	1
DS1=T1	1.544 Mbps	24	24 canales
DS2=T2	6.312 Mbps	96	4xT1
DS3=T3	44.736 Mbps	672	7xT2
DS4=T4	139.264 Mbps	2016	3xT3

Tabla 1.5.2 Jerarquías de transmisión PDH para la norma americana T1

La primer jerarquía T1 se compone de 24 canales a 64 kbps mas un canal de 8 kps usado para señalización, esto totaliza una velocidad de 24*64+8 = 1544 kbps. Las jerarquías T1 son estándares de transporte de EU.

Algunas de las debilidades de PDH son:

- La falta de un estándar mundial en el formato digital, por lo que los estándares europeo y estadounidense son incompatibles.
- No tiene un estándar mundial para interfaces ópticas, por lo que no se puede realizar la interconexión en el ámbito óptico.
- La estructura asíncrona de multicanalización es muy rígida.
- Tiene muy poca capacidad de administración.

Debido a las desventajas de PDH en el ámbito óptico surgió otra técnica de multicanalización, SONET/SDH.

Infraestructura SDH/SONET

La infraestructura SDH/SONET esta definida por la ITU (Internacional Telecomunicatios Union) y por la ANSI (American Nacional Standards Institute) respectivamente. SDH es el estándar Europeo y SONET es el estándar Americano. Ambos son estándares para transmisión digital por fibra óptica. Fueron diseñados para cubrir las deficiencias de compatibilidad de los sistemas de transmisión PDH, además son estructuras escalables que permiten la incorporación de otras tecnologías de redes ópticas y de banda ancha. Los enlaces SONET/SDH son muy seguros debido a su topología de anillo, con lo cual se tiene enlaces redundantes por si alguna fibra se corta, entonces la transmisión continuara por el enlace de respaldo y la comunicación se restaurara en un margen de 50 milisegundos. La especificación SONET/SDH define el formato de la trama, el método de multicanalización y sincronización entre el equipo, así como la especificación de la interfaz óptica.

Las ventajas de SONET/SDH son:

- Se constituye como un estándar mundial en formato digital y para interfase óptica
- Abaratamiento de costos de la red por su compatibilidad transversal. Además de que es compatible hacia delante y hacia atrás.
- Su estructura de multicanalización de sincronía es muy flexible.
- El numero reducido de interfases conectadas espalda con espalda mejoran la confiabilidad y desempeño de la red.
- Tiene gran capacidad de administración.
- Proporciona a los proveedores de servicios de telecomunicaciones más ancho de banda para transportar trafico de voz y datos que la tecnología PDH.

Jerarquías de transmisión por fibra óptica SDH de la norma Europea.

La jerarquía SDH (Synchronous Digital Hierarchy) tiene definidas las velocidades de transmisión para señales eléctricas y ópticas con una tasa base y de incremento de 155.52 Mbps, cada nivel de servicio se conoce como STM-n, STM por sus siglas en ingles es Synchronous Transport Module (Synchronous Transport Module).

Las jerarquías para mayores velocidades de SDH usan desde 1980 canales conocida como STM-1 hasta 120000 canales conocida como STM-64, estas se muestran en la tabla 1.5.3.

Nombre Jerarquía SDH Europea (transmisión eléctrica y óptica)	Velocidad en bits	Canales	Capacidad
STM-1	155.52 Mbps	1980	1xSTM-1
STM-4	622.08 Mbps		4xSTM-1
STM-16	2,488.32 Mbps		4xSTM-4
STM-64	9,953.28 Mbps		4xSTM-16
STM-256	39,813.12 Mbps	120000	4xSTM-64

Tabla 1.5.3 Jerarquías de transmisión para la norma Europea SDH.

Jerarquías de transmisión por fibra óptica SONET de la norma Americana.
La jerarquía SONET tiene definidas las velocidades de transmisión para señales eléctricas en el dominio del tiempo en incrementos de 51.84 Mbps, cada nivel se conoce como STS-n (Synchronous Transport Signal)
También SONET tiene definidas las velocidades de transmisión para señales ópticas en incrementos de 51.84 Mbps, conocido cada nivel como OC-n (Optical Carrier)
Por lo tanto la tasa de transmisión base para SONET (STS y OC) es de 51 Mbps
Estas se muestran en la tabla 1.5.4.

Nombre Jerarquía SONET (transmisión eléctrica)	Nombre Jerarquía SONET (transmisión óptica)	Velocidad en bits	Capacidad
STS-1	OC-1	51.84 Mbps	1 OC-1
STS-3	OC-3	155.52 Mbps	3xOC-1
STS-12	OC-12	622.08 Mbps	4xOC-3
STS-48	OC-48	2,488.32 Mbps	4xOC-12
STS-192	OC-192	9,953.28 Mbps	4xOC-48
STS-768	OC-768	39,813.12 Mbps	4xOC-192

Tabla 1.5.4 Jerarquías de transmisión para la norma Americana SONET

Tanto PDH como SDH/SONET son modelos de redes de conmutación de circuitos basados en voz que transportan millones de circuitos entre varios puntos de conmutación.

Estándares E1/T1

Los estándares E1 y T1 son interfaces TDM. Dependiendo si usan señalización trabajan en la capa de enlace de datos, si no usan señalización o sea únicamente transmiten un flujo de bits trabajan en la capa física.

Estándar E1

La primer jerarquía de un E1 esta compuesta de 32 canales de 64kbps, cada canal es una fracción del E1 y se conoce como E0, los 32 canales hacen un total de 32*64kbps = 2048 kbps (2.048 Mbps) de capacidad de transmisión. De estos 32 canales dos no se usan para transmitir datos, se usan para la sincronización de tramas y señalización, el formato de una trama E1 se muestra en la Fig. 1.5.22

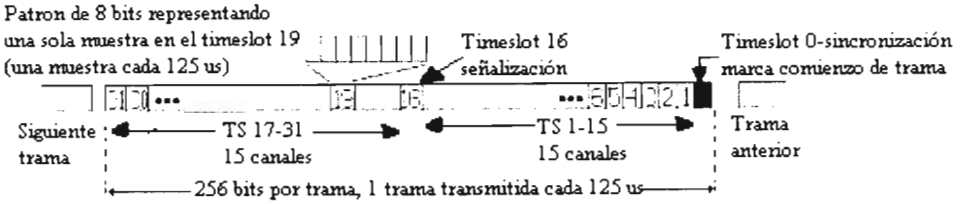


Fig. 1.5.22 Formato de una trama digital de un E1-2.048 Mbps

La Fig. 1.5.21 nos indica que una trama E1 es de 256 bits divida en 32 Time Slots (TS) con 8 bits por cada TS.. Los canales están en TS consecutivos numerados del 0 al 31. La velocidad de cada trama en Hz. es 1/125μs = 8 Khz.

Los TS 1-15 y 17-31 son usados para transmitir los datos de usuario y se conocen como canales 1-30.

El TS0 es usado para tareas de sincronización, alarmas y mensajes.

El TS 16 es usado para tareas de señalización, pudiendo ser usado también para transmitir datos.

El formato agrega una multitrama formada con 16 tramas consecutivas numeradas del 0-15, se usa para agregar información acerca de los datos. Estas 16 tramas en el TS 0 proporcionan información acerca de la sincronización y la corrección de errores, esta es obtenida de todas las tramas pares, donde el patrón de sincronización que se usa es 0011011, este patrón es contenido en los bits 1-7 (0-7) de las tramas numeradas pares (0, 2,..), esta sincronización no involucra un reloj, sino que los bits son transmitidos aun con la línea desocupada.

El chequeo de errores es realizado con una comprobación de redundancia cíclica (CRC-4) que usa 4 bits por cada mitad de la multitrama (8 tramas) antes que el patrón de sincronización, los bits de indicación de errores usando CRC-4 están contenidos en las tramas 13 y 15. El bit de indicación de alarma remota esta contenido en el bit 3 de las tramas numeradas impares. Otros bits en las tramas impares son los bits de reserva. Esto se observa en la tabla 1.5.5:

Bits C1-C4 para comprobación CRC-4

#Trama #Bit	0	1	2	3	4	5	6	7
0	C1	0	0	1	1	0	1	1
1	0	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
2	C2	0	0	1	1	0	1	1
3	1	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
4	C3	0	0	1	1	0	1	1
5	1	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
6	C4	0	0	1	1	0	1	1
7	0	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
8	C1	0	0	1	1	0	1	1
9	1	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
10	C2	0	0	1	1	0	1	1
11	1	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
12	C3	0	0	1	1	0	1	1
13	Error Set	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva
14	C4	0	0	1	1	0	1	1
15	Error Set	1	Alarma	Reserva	Reserva	Reserva	Reserva	Reserva

Bits de Sincronización

Sub multitrama

Indicación de alarma remota

Tabla 1.5.5 Estructura de una multitrama del TS0 en un E1

En el TS 16 la multitrama proporciona información acerca de la señalización. Cuando se tiene señalización por canal común (CCS) al menos un canal, el TS 16 es usado para

sincronización y sirve asincrónicamente a todos los canales. Cuando se tiene señalización por canal común, en cada multitrama para cada uno de los canales, hay una mitad de trama del TS16 que esta dedicada para esa señalización de canal, así:
La trama 0 se usa para indicación de alarma y bits de reserva.
La trama 1 es usada para los bits 1 y 16 usando 4 bits por cada uno.
La trama 2 es usada para los bits 2 y 17 usando 4 bits por cada uno.
La trama 15 es usada para los bits 15 y 30 usando 4 bits por cada uno.

Estándar T1

Estructura de la trama T1
La trama T1 esta compuesta de 24 canales que se representan en time slots numerados del 0-23. Cada canal de 64 kbps es una fracción del T1 y se conoce como DS0. La trama es de 193 bits, se compone de 1 bit de entramado + 8 bits * 24 time slots, el bit de entramado crea un canal adicional de 8 kbps. La velocidad de las tramas es de 8 Khz.

Estructura de la supertrama T1
La supertrama esta compuesta de 12 tramas numeradas del 1-12, incluye un mecanismo de sincronización con patrón de 001001 y puede incluir un mecanismo de señalización, estos mecanismos usan el bit de entramado que es agregado a cada trama y pueden ser usados para limitar tramas y supertramas. La señalización CAS es opcional la cual usa dos bits por cada canal, 1 bit de la 6ª trama y de la 12ª trama por lo que cada canal pierde 2 bits en cada supertrama, así se forma un canal de 10.666 kbps, de acuerdo a esto la velocidad de los canales decrece de 64 kbps a 56 kbps, esto lo podemos ver representado en las tablas 1.5.6 y 1.5.7

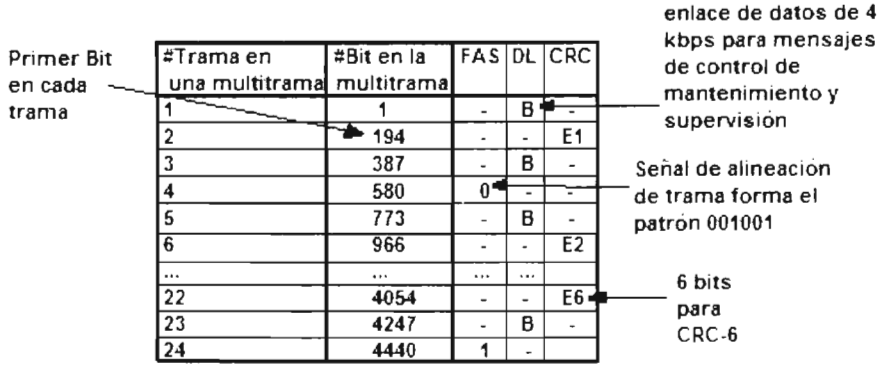
Patrón de sincronización para la trama

Patron de sincronización para la supertrama

#Trama	Limites de trama	Limites de supertrama	Bits de información
1	1	-	1-8
2	-	0	1-8
3	0	-	1-8
4	-	0	1-8
5	1	-	1-8
6	-	1	1-8 1-7+1 CAS
7	0	-	1-8
8	-	1	1-8
9	1	-	1-8
10	-	1	1-8
11	0	-	1-8
12	-	0	1-8 1-7+1 CAS

La señalización de canal asociado esta usando 2 bits en cada canal

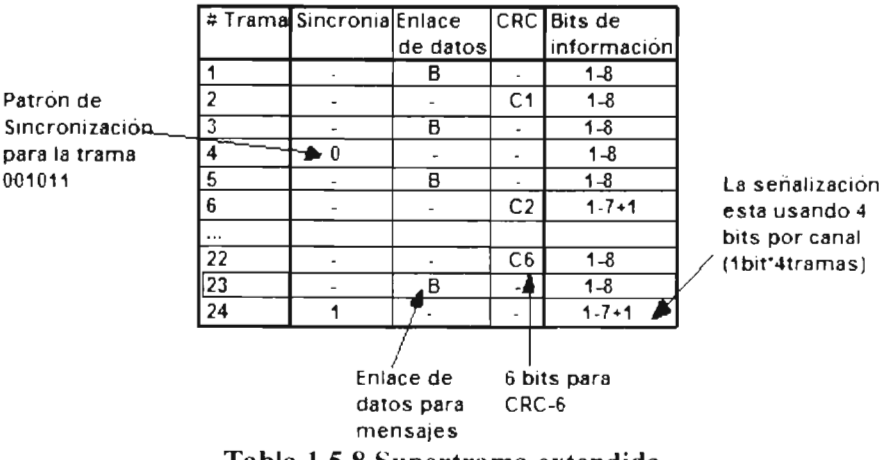
Tabla 1.5.6 Estructura de la supertrama T1



#Trama en una multitrama	#Bit en la multitrama	FAS	DL	CRC
1	1	-	B	-
2	194	-	-	E1
3	387	-	B	-
4	580	0	-	-
5	773	-	B	-
6	966	-	-	E2
...	...	...	...	
22	4054	-	-	E6
23	4247	-	B	-
24	4440	1	-	

Tabla 1.5.7 Bit de entramado de la supertrama del T1

El formato T1 tiene una supertrama extendida que se componen de 24 tramas, para señalización usa un bit cada 6 tramas (6, 12, 18, 24) por cada canal, se conoce como señalización A/B/C/D. Esta supertrama tiene tres tipos de información de entramado que son:
La sincronización que usa el patrón 001011 cada 4 tramas (4, 8, 12, 16, 20, 24).
CRC-6 cada 4 tramas a partir de la 2ª (2, 6, 10, 14, 18, 22), se usa para detectar todos los errores de menos de 6 bits y 98.4% de errores en los demás bits, también previene la perdida de sincronización que se pudiera dar por patrones idénticos al de sincronización.
Enlace de datos en las tramas impares 1, 3, 5,....23 creando un canal de 4 kbps para control de mantenimiento y supervisión, tabla 1.5.8



# Trama	Sincronia	Enlace de datos	CRC	Bits de información
1	-	B	-	1-8
2	-	-	C1	1-8
3	-	B	-	1-8
4	0	-	-	1-8
5	-	B	-	1-8
6	-	-	C2	1-7+1
...				
22	-	-	C6	1-8
23	-	B	-	1-8
24	1	-	-	1-7+1

Tabla 1.5.8 Supertrama extendida

1.6 Códigos de transmisión

En los sistemas de comunicación digitales la información a transmitir tiene que ser adaptada al medio de transmisión. Para esto será preciso codificarla de manera que pueda asegurarse una recepción adecuada y segura.

Codificación
Genéricamente hablando la codificación es la correspondencia de los símbolos de información de un alfabeto fuente y una secuencia de símbolos de un alfabeto destino. Al alfabeto destino se le llama alfabeto código y a cada una de las secuencias de símbolos de este alfabeto que corresponda con un símbolo del alfabeto fuente se le llama palabra de código. Una representación grafica de esto se puede ver en la Fig.1.6.1

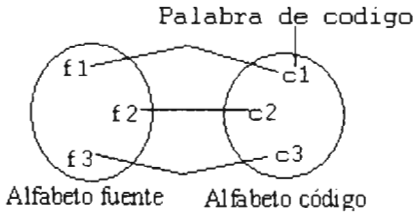


Fig. 1.6.1 Representación de la codificación

El alfabeto fuente contiene los símbolos originales que se quieren codificar. El alfabeto código tiene las palabras de código equivalentes en que se codificaran los símbolos originales. Estas palabras de código son aptas para ser transmitidas por un sistema de comunicaciones.
La codificación digital es el conjunto de técnicas que se usan para representar los bits de datos utilizando señales analógicas o digitales, estas técnicas transforman los datos o información en algo representativo de esa información y que es apto para su transmisión por un medio cualquiera. Así en las comunicaciones digitales los bits se transforman en algo tangible, físico como un pulso eléctrico en un cable, un pulso luminoso en una fibra óptica, o un pulso de ondas electromagnéticas en el espacio.
La codificación en forma practica es la transformación de los trenes de bit lógicos compuestos de 0´s y 1´s representados como corriente continua a una forma alternada o de corriente alterna sobre la base de los sistemas de codificación creando de esta forma ondas pulsantes basadas en las series de Fourier.
La codificación con señales de corriente continua puede usar diversos métodos desde la más básica como la representación de un bit 1 con un determinado voltaje 3-5 volts y un bit 0 con un voltaje menor o 0 volts. El problema con estas señales de corriente continua es que pierden rápidamente potencia por que solo son adecuadas en el caso de pequeñas distancias, además cuando los trenes deben ser transportados por diferentes redes o cableados se hace mediante corriente alterna.
Por su parte en la codificación con señales de corriente alterna (señales analógicas) se tiene el inconveniente de que la corriente va variando entre dos valores extremos con el tiempo por lo que no podemos usar el sistema aplicado en el caso de corriente continua a no ser que se pudiera variar la forma ondulante de la corriente alterna en una forma pulsante como se observa en la Fig. 1.6.2 con lo que podríamos obtener señales parecidas a las conseguidas en el caso de corriente continua, las ondas alternas pulsantes son lo que conocemos como señales digitales.

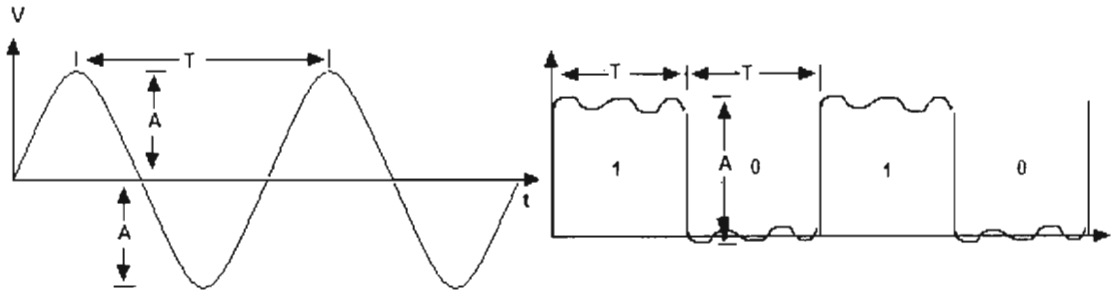


Fig. 1.6.2 Señales pulsantes

Esta necesidad de transformación se realiza sobre la base del teorema de Fourier con el cual un pulso rectangular se puede generar usando la combinación correcta de ondas sinusoidales como se realiza en la Fig. 1.6.3.

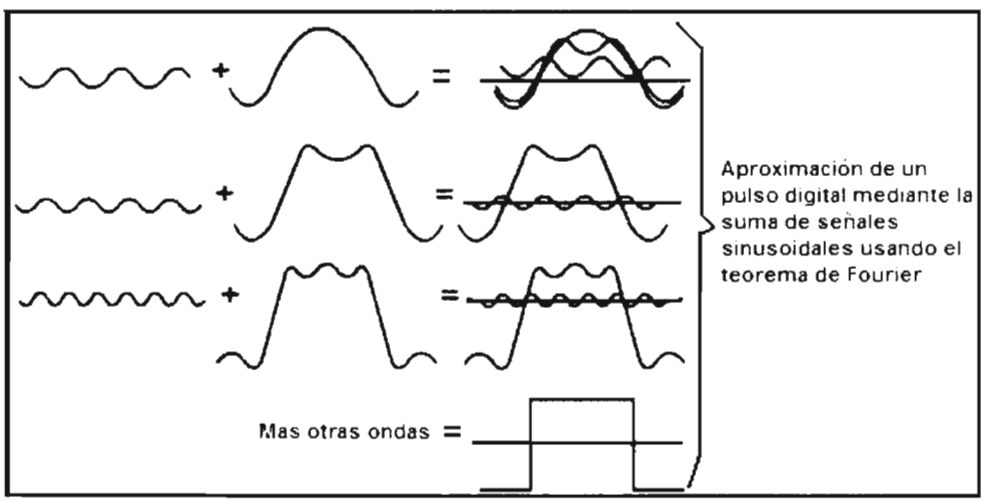


Fig. 1.6.3 Señales de fourier para un pulso digital

La codificación es usada para transmitir los datos digitales mediante diferentes códigos de transmisión que se conocen como códigos de línea. Existen códigos como encendido-apagado, polar, bipolar, etc. Se debe utilizar un buen esquema de codificación para mejorar las prestaciones del sistema de transmisión, dicho esquema de codificación debe establecer una correspondencia entre los bits de datos y los elementos de la señal.

Código

El código es la correspondencia que existe entre cada símbolo del alfabeto fuente y cada conjunto de símbolos.

Por lo tanto un código es un acuerdo sobre un conjunto de significados que definen una serie de símbolos y caracteres. Así existen combinaciones de bits que representan un carácter dentro de una tabla de códigos.

En los sistemas de comunicaciones tenemos tres tipos de codificación: codificación en la fuente, codificación de compresión y codificación de línea.

- Codificación de información en la fuente. El objetivo de esta codificación es hacer una representación eficiente de los símbolos del alfabeto fuente, esto se

realiza eficientemente sobre la base del conocimiento de la probabilidad de cada símbolo fuente. El código que se utilizó en las primeras transmisiones telegráficas y radioeléctricas fue el código Baudot. El cual consistía de una tabla de códigos de 5 bits que representaban 32 caracteres distintos, dos de estos conmutaban entre las letras mayúsculas del abecedario (A-Z) y figuras (0-9, signos de puntuación y caracteres especiales hasta un total de 26). También tenemos el código BCD (Binary Coded Decimal) usado para representar datos en notación binaria para poder ser manejados por computadoras, permite codificar los caracteres alfanuméricos mediante 6 bits. Del BCD se derivo el EBCDIC (Extended Binary Coded Decimal Interchange Code) que utiliza 8 bits para poder utilizar caracteres de control en la manipulación de mensajes y otras funciones. El código FIELDDATA de 6 bits manejaba hasta 64 símbolos, se aplicaba en transmisiones militares y estaba orientado al lenguaje maquina. El código ASCII (American Standard Code for Information Interchange) de 7 bits es capaz de manejar hasta 128 caracteres, es usado principalmente para facilitar el intercambio de información entre sistemas de procesamiento de datos y equipos asociados dentro de sistemas de comunicación de datos.. El código ASCII incremento el numero de bits a 8 para representar los 128 caracteres del código de 7 bits mas otros 128 caracteres para que cada fabricante pudiera ampliar sus propios caracteres. Aunque cabe hacer notar que en las transmisiones entre equipos diversos no es recomendable usar caracteres de la ampliación debido a los errores de interpretación que se pueden generar.

- Codificación de compresión. Los códigos de compresión se usan para reducir el tamaño de los datos sin alterar el significado de la información que contienen.
- Códigos de línea. Codifican en forma digital a los bits para poder ser transmitidos por el medio. Definen la relación entre los bits y los pulsos de la señal a transmitir.

Codificación de línea

Es la asignación de formas de onda arbitrarias para los unos y ceros resultantes del muestreo y cuantificación de señales, estas formas de onda influirán en la potencia de transmisión, ancho de banda, facilidad de recuperación del reloj en el receptor, detección y corrección de errores.

Los códigos de línea Fig. 1.6.4 o códigos autosincronizados incorporan la temporización a la propia señal en vez de usar un canal de sincronismo aparte, esto es muy importante para cuando las distancias de transmisión son muy grandes, ya que el envío de la señal de sincronía en un canal aparte de los datos provoca que se desfasen, dificultando al receptor la sincronización de los datos. El código autosincronizado permite determinar el momento exacto en que llega un bit, para lograr esto la línea debe cambiar de estado en forma continua. Los mejores códigos autosincronizados son aquellos en los que el estado de la línea cambia frecuentemente. Lo que hace el reloj es proporcionar la referencia para los unos y ceros individuales.

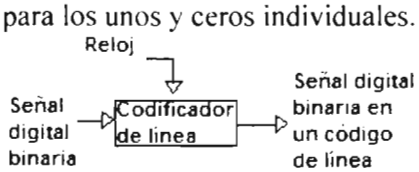


Fig. 1.6.4 Codificación de línea.

Los códigos de línea o códigos autosincronizados deben tener las siguientes propiedades para tener un buen sistema de codificación:

1. Contenido adecuado de sincronización. Debe ser posible extraer la información de sincronización o de reloj de la señal, esta señal hará la separación de un bit respecto a otro, la señal de reloj puede ser una señal separada lo cual es muy costoso y hace lenta la transmisión o bien la propia señal puede transportar la sincronización, esto implica un sistema de codificación adecuado y muchos cambios en el voltaje para permitir la sincronización aprovechando los cambios en el nivel de voltaje.
2. Un pequeño ancho de banda para permitir a muchas señales ser transmitidas sobre un canal de comunicación dado.
3. Eficiencia. Para un ancho de banda y una potencia de transmisión dados, el código debe tener la mínima probabilidad de error de detección, o sea la máxima inmunidad al ruido del canal y a la interferencia intersimbólica.
4. Señal no polarizada para que al pasarla sobre un cable de 2 hilos no sea afectada por la conexión física de los hilos.
5. Capacidad de detección y de corrección de errores. Debe detectar y si es posible corregir el error en la detección. En un código bipolar por ejemplo, un solo error ocasionaría violación bipolar y puede ser detectado fácilmente.
6. Densidad espectral de potencia favorable. Se debe concentrar la energía de la señal en el centro de la banda de frecuencias para que las interferencias sean las menores posibles. El espectro de frecuencia de la señal debe igualarse a la respuesta de frecuencia del canal, ya que si un canal tiene mucha atenuación en las frecuencias mas bajas, el espectro de la señal debe tener una densidad espectral de potencia pequeña dentro de este rango para evitar excesiva distorsión de la señal. Asimismo la densidad espectral de potencia debería ser cero cuando la frecuencia w=0 (componente de corriente directa cd), ya que el acoplamiento a corriente alterna (ca) se usa en los repetidores. Si se tiene mucha potencia en los componentes de baja frecuencia, la cd vagara dentro de la corriente de pulsos cuando se use el acoplamiento a ca. Por lo tanto se deben tener bajos niveles de señal de dc para que no sean atenuadas las señales y puedan ser transmitidas a grandes distancias. Así en un sistema de banda base se busca que el espectro no contenga componentes de DC, ni componentes de baja y alta frecuencia.
7. Transparencia. Transmisión correcta de una señal digital independientemente del patrón de 1´s y 0´s. Una larga sucesión de ceros puede ocasionar errores en la extracción de temporización. Si los datos se codifican de manera que para toda sucesión de datos la señal codificada se reciba fielmente, el código será transparente.
8. Inmunidad al ruido e interferencias. Usar códigos más inmunes al ruido, los cuales son códigos más robustos para el ruido.
9. Muchos cambios en el voltaje para permitir la sincronización entre el emisor y el receptor sin necesidad de agregar información extra y que permita la extracción de la señal de reloj.
10. Coste y complejidad. Aumentando la razón de elementos de la señal aumentara el coste del sistema.

Concretamente la codificación de los datos permitirá al transmisor conocer:

- El tiempo empleado en enviar un bit, este tiempo es obtenido si se conoce la tasa de transmisión, si es de n bps entonces la duración de un bit será 1/n segundos
- La velocidad de modulación (o transmisión de pulsos) la cual es dada en baudios

En la recepción permitirá conocer:

- La duración de cada bit
- El comienzo y fin de cada bit.
- Los niveles de tensión usados para representar cada bit.

A continuación tenemos algunos códigos de línea:

- Codificación NRZ Unipolar

La codificación NRZ (Non Return to Zero), Fig. 1.6.5 es una codificación sin retorno a cero por que el nivel del 1 o el 0 es constante durante todo el intervalo de duración del bit (es decir no vuelve a cero durante el intervalo).

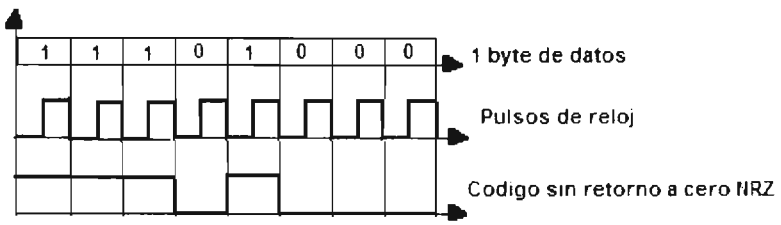


Fig. 1.6.5 Código NRZ unipolar

Sus características son:
- Cuando se tienen bits de valor 1 consecutivos la señal no tiene alternancia de voltaje.
- Es una señal de tipo unipolar por que el voltaje que representa a los datos digitales varia entre 0 y +V volts o sea el voltaje siempre es del mismo signo.
- Es uno de los tipos de codificación más sencillas, ya que solo tiene una señal alta y una baja (normalmente +5 o +3.3 V para representar un bit 1 y 0 V para el bit 0 o al revés, desprecia las transiciones).
- Es una forma de onda comúnmente usada en computadoras.

Sus ventajas son:
- Es una codificación muy sencilla, de fácil implementación, hace un uso eficiente del ancho de banda puesto que representa un bit con cada baudio.

Sus desventajas son:
- Tiene un alto nivel de componentes de corriente continua, es inadecuado para grandes distancias debido a los residuos de corriente continua, tiene un promedio de ½ V para una secuencia conteniendo el mismo numero de 1´s y 0´s.
- Puede presentar posibles ausencias de suficientes transiciones de señal dificultando la sincronización entre el emisor y el receptor, es un código demasiado limitado para la transmisión de señales.

- Código NRZ polar.

Este código desplaza el nivel de referencia de la señal al punto medio de la amplitud de la señal, Fig. 1.6.6, es polar por que el 1 y 0 tiene representaciones opuestas o signos diferentes. Con esto reduce a la mitad la potencia requerida para transmitir la señal en comparación con la unipolar.

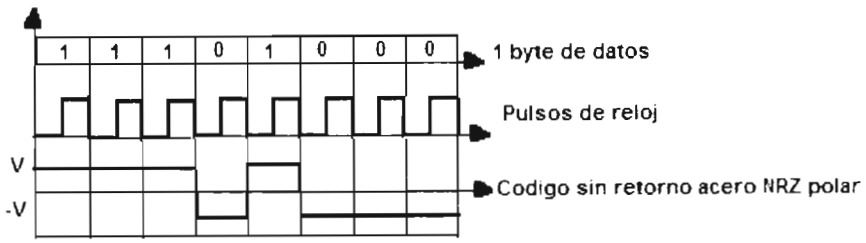


Fig. 1.6.6 Código NRZ polar

- Código RZ unipolar.

El código de retorno a cero (Return to Zero) representa los valores de un bit 0 con 0 volts, un bit 1 con +V durante la primera mitad del bit y un valor 0 en la segunda mitad (es decir regresa a cero a la mitad del bit 1), Fig. 1.6.7.

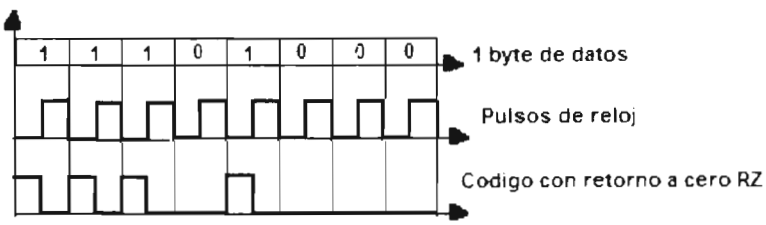


Fig. 1.6.7 Código RZ unipolar

Sus características son:

- Este método tiene un promedio de voltaje de DC de solo ¼ de volt.
- Tiene buenas características de sincronización ya que aun cuando se tengan bits 1 consecutivos existen cambios de voltaje para efectuar la sincronía.
- El máximo ancho de banda es la velocidad de datos en si misma para una secuencia conteniendo solo 1´s.
- Como se requieren dos transiciones de señal por cada bit requiere el doble del ancho de banda que el código NRZ.

- Código RZ polar.

El código de retorno a cero polar representa los valores de un bit 0 con -V volts, un bit 1 con +V durante la primera mitad del bit y un valor 0 en la segunda mitad (es decir regresa a cero a la mitad del bit 1), Fig. 1.6.8.

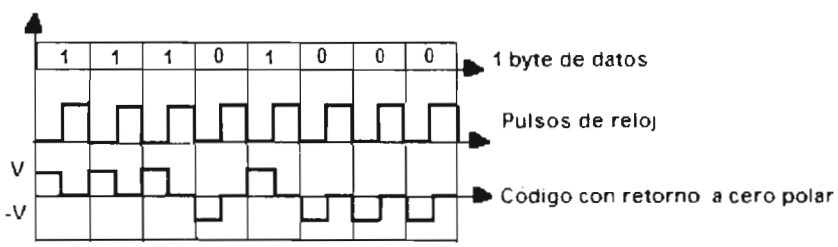


Fig.1.6.8 Código RZ polar

- Código NRZI.

El código NRZI (Non Return to Zero Invertive) es una modalidad del código NRZ en el cual se codifican los bits cuando se producen cambios de tensión. Sabiendo la duración de un bit, un 1 se codifica con un cambio de tensión 0 o +V volts. Si el voltaje previo fue 0 volts el actual será +V volts, por otro lado si el voltaje previo fue +V volts el actual será 0 volts. Un 0 se codifica con 0 volts o sin cambio, Fig. 1.6.9.

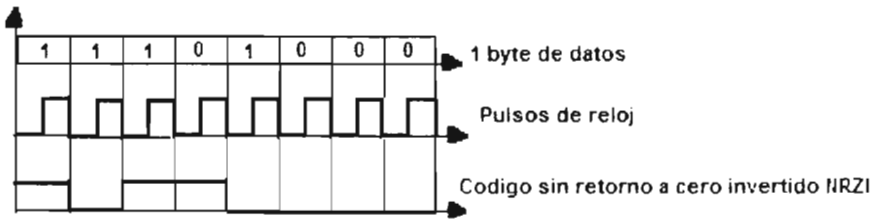


Fig. 1.6.9 Código NRZI

Este código se conoce también como una codificación diferencial, ya que compara la polaridad de los elementos de señal adyacentes y esto hace posible detectar mejor la presencia de ruido y es más difícil perder la polaridad de una señal cuando hay dificultades de transmisión. Combina el ancho de banda más pequeño de NRZ y los cambios de frecuencia en el voltaje RZ además de que agrega la ventaja de ser una señal no polarizada.

- Código de Manchester.

El código Manchester, Fig. 1.6.10, se basa en realizar cambios de transición de estado con cada bit, pudiendo haber hasta dos. Así un 0 lo codifica como una transición de baja a alta y el 1 se codifica como una transición de alta a baja, dichas transiciones se realizan a la mitad de la duración de cada bit con lo que la mitad del bit se encarga de la sincronización. Debido a que tanto los 0 y los 1 dan como resultado una transición en la señal, el reloj se puede recuperar eficazmente en el receptor proporcionando una buena sincronización por los constantes cambios de nivel.

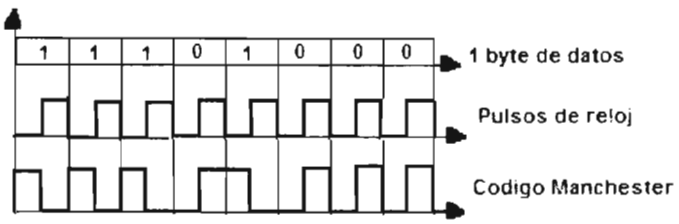


Fig.1.6.10 Código Manchester

Algunas de sus características son:

- Este código no tiene componente en continua.
- Detecta muy bien los errores, tiene un mejor comportamiento frente al ruido.
- La velocidad de transmisión será el doble que en el código NRZ, su gran desventaja es el gran ancho de banda utilizado.

- Código Manchester Diferencial.
Utiliza la transición en mitad del intervalo solo para realizar la sincronización, la presencia de un cambio de voltaje al inicio del bit es lo que indica la presencia de un 1. Si existe un 0 habrá una transición de menos a más (o al revés) tanto al principio como a la mitad del intervalo. Si existe un 1 habrá una transición de mas a menos (o al revés) en la mitad del intervalo, Fig. 1.6.11 Este código detecta muy fácilmente los errores de transmisión.

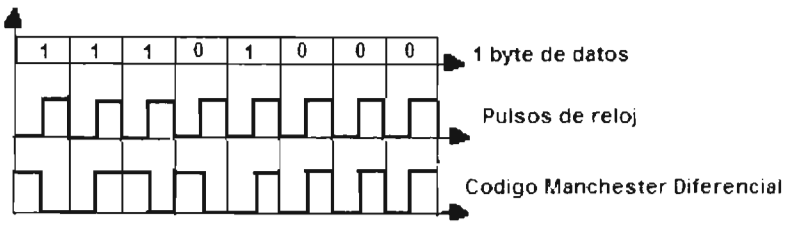


Fig. 1.6.11 Código Manchester diferencial

Los Códigos Manchester son auto sincronizados ya que el receptor se sincroniza usando la transición obligatoria de cualquier bit, no hay componente de CD, detecta fácilmente los errores ya que la no transición en la mitad de un intervalo supone un error fácil de detectar. Son populares para redes de distancias cortas, como la transmisión de datos con código Manchester en ethernet, no son buenos para distancias largas debido a la alta velocidad de elementos de señal que requieren comparada con la velocidad de los datos que ofrece.

- Código PE.
El código PE (Phase Encoding Manchester), Fig. 1.6.12, representa los datos digitales como sigue:
Los bits 0 con un voltaje de +V volts en la primera mitad del bit y –V volts en la segunda.
Los bits 1 con un voltaje de –V volts en la primera mitad del bit y +V volts en la segunda.

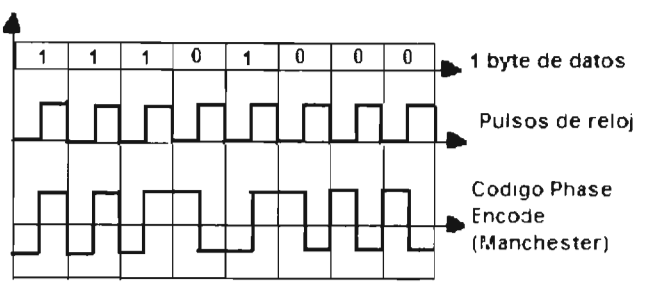


Fig. 1.6.12 Phase Encoding (Manchester)

Este método tiene todas las ventajas necesarias pero requiere gran ancho de banda y la polaridad de la señal

- Código CDP.
CDP (Conditional Diphase) combina los métodos NRZI y el PE como sigue:
El bit 0 es representado por un cambio de voltaje en la misma dirección del bit previo (y la transición se hace de +V a –V o de –V a +V).

El bit 1 es representado por un cambio de voltaje en la dirección opuesta del bit previo (y la transición es de +V a –V o de –V a +V), la Fig. 1.6.13 muestra el código CDP. Este método no es sensible a la polarización de la señal.

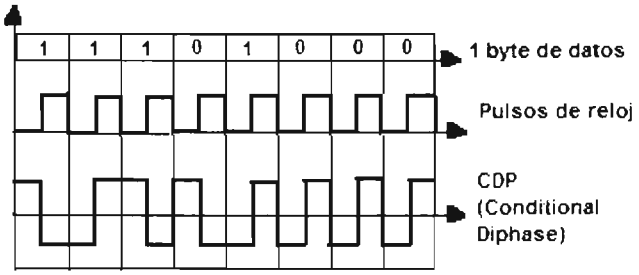


Fig. 1.6.13 CDP Condicional Diphase

- Codificación Binaria multinivel.

Esta codificación intenta subsanar las deficiencias de la codificación NRZ usando mas de dos niveles de señal, para esto codifica un 1 cada vez que se produce un cambio de nivel de señal y codifica un 0 cuando no hay cambio de nivel de señal, aunque esto tiene problemas cuando se tiene una cadena de ceros. Tiene las ventajas de que no hay problemas de sincronización con cadenas de 1, no hay componente en continua, ocupa un ancho de banda menor que el NRZ y la alternancia de pulsos permite la detección de errores. Presenta los problemas con cadenas de 0, es menos eficaz que el NRZ y tiene una mayor tasa de errores.

- Transmisión bipolar o AMI(Alternate Mark Inversion).

El código de inversión de marcas alternadas AMI es uno de los mas empleados en la transmisión digital ya que no tiene componente de corriente continua residual debido a la transición que se produce cada vez que hay un 1 y su potencia a frecuencia cero es nula. Se llama bipolar por que el voltaje puede ser positivo o negativo. Codifica un bit 1 como un voltaje positivo y como un voltaje negativo alternado, el símbolo 0 con ausencia de señal, Fig. 1.6.14. Para realizar esto se transmiten pulsos con un ciclo de trabajo del 50% e invirtiendo alternativamente la polaridad de los bits 1 que se transmiten.

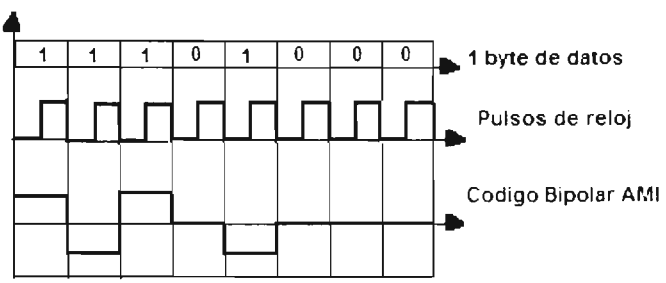


Fig. 1.6.14 Código Bipolar AMI

Algunas de sus características son:

- Constituye un medio para que el emisor y receptor permanezcan sincronizados a pesar de que se produzcan largas cadenas de 1's.
- Permite detectar errores en la transmisión muy fácilmente ya que si existen dos valores positivos sin alternancia entre ellos serán interpretados como un error en la línea, los 0 son espacios sin presencia de voltaje.
- Este formato bipolar es una señal de tres estados +V, 0 y –V.

- El ancho de banda se reduce significativamente con respecto a NRZ.
- Este código al igual que otros tiene la desventaja de que la presencia de ceros continuos darán problemas para la sincronización.

- Pseudo ternario.
Este código es el inverso del AMI, por lo que tiene las mismas propiedades. Cuando hay un 1 no hay señal, cuando hay un 0 manda un pulso positivo o negativo de forma alternada, Fig. 1.6.15

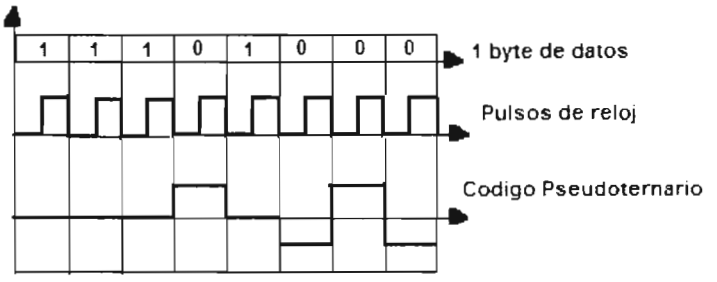


Fig. 1.6.15 Código Pseudo ternario

Códigos con técnicas de altibajos
Estos códigos sustituyen secuencias de bits que provocan niveles de tensión constantes por otras que garantizan la anulación de la componente continua y la sincronización del receptor, estas sustituciones provocan violaciones bipolares. La longitud de la secuencia no se altera, por lo que la velocidad de transmisión de datos es la misma, el receptor debe ser capaz de reconocer estas secuencias de datos especiales. Básicamente existen dos técnicas y se basan en el AMI bipolar:

- Técnica BNZS.
  En esta técnica los códigos llamados genéricamente BNZS se crearon para tratar de solucionar los problemas de sincronización que provocan largas secuencias de 0's.
- Códigos mBnL, estos códigos buscan representar mas de un bit con el mismo pulso. Por lo que una secuencia de m Bits se transmiten como n pulsos de señal (m>n).

- **Códigos BNZS.**

- B6ZS
Esta codificación sustituye 6 0's consecutivos según la tabla 1.6.1 dependiendo de la polaridad del pulso precedente a los ceros.

Pulso de voltaje anterior a los 6 ceros	Sustitución de los 6 ceros por
Positivo	0+-0-+
Negativo	0-+0+-

Tabla 1.6.1 Codificación B6ZS

Se usa en los sistemas T2 que trabajan a 6.312 Mbps, Fig. 1.6.16

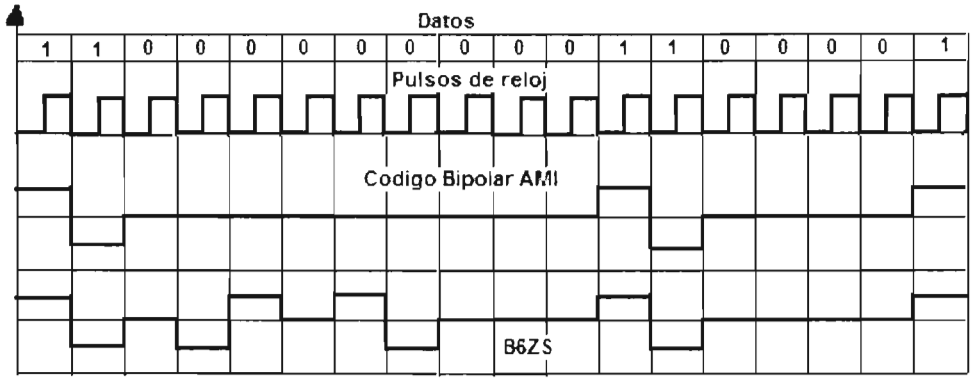


Fig. 1.6.16 Código B6ZS

- B8ZS.

La codificación B8ZS (Bipolar with 8-Zeros Substitution) sustitución bipolar con 8 ceros es la mas usada principalmente en Estados Unidos. Codifica los datos sobre la base del código bipolar AMI y cuando encuentra ocho 0´s consecutivos los sustituye por alguna secuencia según la tabla 1.6.2, según si el pulso anterior fue positivo o negativo.

Valor del voltaje anterior a los 8 ceros	Sustitución de los 8 ceros por
Positivo	000+-0-+
Negativo	000-+0+-

Tabla 1.6.2 Sustituciones B8ZS

Este código se observa en la Fig.1.6.17.

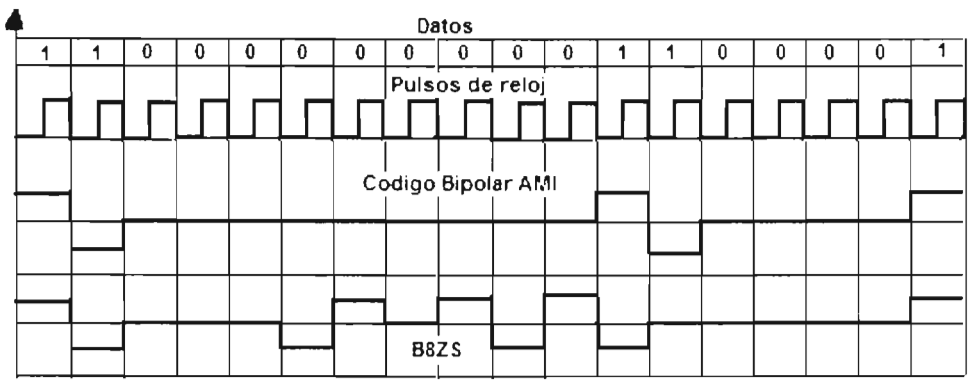


Fig. 1.6.17 Código B8ZS

-HDB3.

La técnica HDB3 (High Density Bipolar-3 Zeros), representa el dato digital casi como el código bipolar AMI y cuando encuentra cuatro 0's consecutivos los sustituye por alternancias según la polaridad del pulso anterior y el numero de 1's según la tabla 1.6.3. No permite mas de tres ceros consecutivos

Valor del voltaje anterior a los cuatro ceros	Números de 1's desde la ultima sustitución	
	PAR	IMPAR
Pulso anterior positivo	-00-	000+
Pulso anterior negativo	+00+	000-

Tabla 1.6.3 Sustituciones HDB3

El funcionamiento de la sustitución de la tabla 1.6.3 es el siguiente:
Cuando hay cuatro bits 0 consecutivos son cambiados por una secuencia conteniendo 000V donde la polaridad del bit V es la misma del pulso anterior no-cero (opuesto a un bit 1 el cual causa una señal V con un voltaje alterno conforme al previo). Hacerlo así el problema de voltaje sin cambios para una secuencia de 0's es resuelta, pero surge un nuevo problema por que la polaridad de los bits no-cero es la misma, un nivel de DC no-cero se formo. Para descartar de este problema la polaridad del bit V es cambiado para ser el opuesto del bit V previo. Cuando esto pasa la secuencia de bits es cambiada otra vez a B00V donde la polaridad del bit B es de la misma polaridad del bit V. Cuando el receptor obtiene el bit B piensa que es un bit 1 pero cuando recibe el bit V (con la misma polaridad) entiende que el bit B y V son de hecho 0.
El funcionamiento de este código se observa en la Fig.1.6.18.

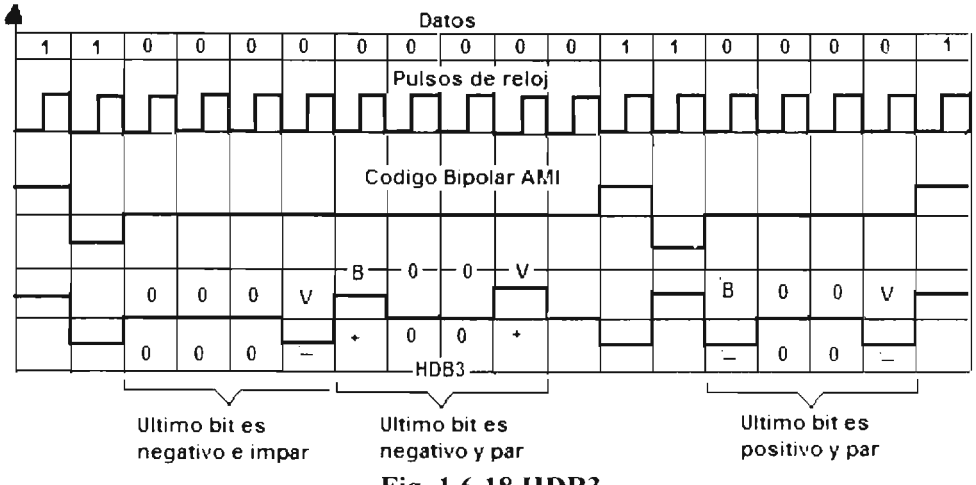


Fig. 1.6.18 HDB3

El método HDB3 cuida todos los requerimientos mientras trata con los problemas que pueden ocurrir.
Estos códigos son adecuados para la transmisión de datos a altas velocidades ya que su espectro es muy estrecho y se concentra en torno a la frecuencia correspondiente a la mitad de la razón de datos.

- **Códigos mBnL.**

También existen códigos de línea para enlaces puramente digitales los cuales tienen la función de eliminar el cross-talk entre pares de hilos adyacentes de diferentes accesos básicos y reducir la densidad espectral de potencia. Se usan para el acceso en la red ISDN. Trabajan a altas velocidades, alrededor de los 160 kbps y trabajan bien en grandes distancias. Son usados para reducir la razón de baudios, esto es, representan mas de un bit con un solo pulso.
Estos códigos son del tipo mBnL (con n<m y L>2) que se leen como m Bits se mapean en n símbolos de un código compuesto de L niveles, o dicho de otra forma una secuencia de m Bits se transmiten como n pulsos de señal. De estos tipos de códigos tenemos el código americano (2B1Q) y el europeo (4B3T).

- Código 4B3T

En el código 4 binario 3 ternario (4B3T), sobre la base de un orden preestablecido 4 bits se mapean en 3 símbolos ternarios, o dicho de otra forma representa cada grupo de 4 bits con 3 pulsos de señal, estos pulsos pueden tener tres niveles de tensión (de ahí el nombre de ternario): positivo, negativo y nulo que se representan como +, - y 0, con esto se tiene una tasa de bits de ¾ de baudio reduciéndose ¼ la tasa original de baudios. Los códigos o pulsos transmitidos para cada 4 bits se obtienen de las columnas S1, S2, S3, S4 de la tabla 1.6.4.

Secuencia Binaria 4B	S1 Código 3T	Sig. Cod.	S2 Código 3T	Sig. Cod.	S3 Código 3T	Sig Cod.	S4 Código 3T	Sig Cod.
0001	0-+	1	0-+	2	0-+	3	0-+	4
0111	-0+	1	-0+	2	-0+	3	-0+	4
0100	-+0	1	-+0	2	-+0	3	-+0	4
0010	+-0	1	+-0	2	+-0	3	+-0	4
1011	+0-	1	+0-	2	+0-	3	+0-	4
1110	0+-	1	0+-	2	0+-	3	0+-	4
1001	+-+	2	+-+	3	+-+	4	---	1
0011	00+	2	00+	3	00+	4	--0	2
1101	0+0	2	0+0	3	0+0	4	-0-	2
1000	+00	2	+00	3	+00	4	0--	2
0110	-++	2	-++	3	--+	2	--+	3
1010	++-	2	++-	3	+--	2	+--	3
1111	++0	3	00-	1	00-	2	00-	3
0000	+0+	3	0-0	1	0-0	2	0-0	3
0101	0++	4	-00	1	-00	2	-00	3
1100	+++	4	-+-	1	-+-	2	-+-	3

Tabla 1.6.4 Tabla de codificación 4B3T

Así para una secuencia de 4 bits y la columna código (S1-S4) se determina el código a transmitir mientras la columna Sig. Cod. nos dice de cual columna se tomara el siguiente código para la siguiente secuencia de 4 bits. Inicialmente se trabaja con la columna 1. Para la Fig. 1.6.19 los primeros 4 bits 1011 se transmitirán como +0- y el

Sig. Cod. se tomara de la columna 1, así para la 2ª secuencia 1001 se transmiten +-+ y el SIG. Cod se toma de la columna 2 y así sucesivamente.

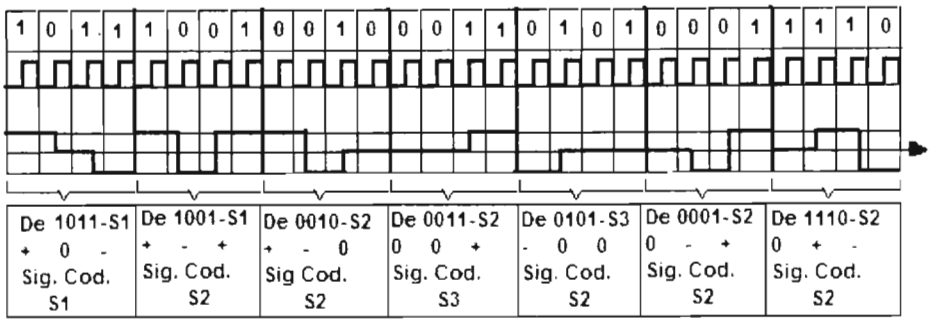


Fig. 1.6.19 Codificación 4B3T

Estos códigos tienen un nivel medio de cd nulo, con lo cual se puede separar la transmisión y recepción, así como evitar errores de interpretación en el receptor facilitando a la vez la transmisión de alimentación por la misma línea.

- Código 2B1Q

El código 2 binario 1 cuaternario (2B1Q), mapea 2 bits en un símbolo quaternario. Mediante la codificación de estos dos bits en cuatro posibilidades, la Q (cuaternario) indica el número de niveles posibles, es decir 4 posibilidades. El código opera tomando los bits binarios dos a dos, y se transmiten como un pulso que toma un valor de 4 niveles de tensión, +1, -1, +3, -3, la regla de codificación sigue la tabla 1.6.5. Las reglas usan un bit para indicar la polaridad (positivo=1, negativo =0) y un bit para indicar la magnitud (1 V=1, 3V=0).

1er bit Bit-polaridad	2° Bit Bit-magnitud	Símbolo Cuaternario
1	0	+3
1	1	+1
0	1	-1
0	0	-3

Tabla 1.6.5 Tabla de codificación 2B1Q

Esta codificación se muestra en la Fig. 1.6.20.

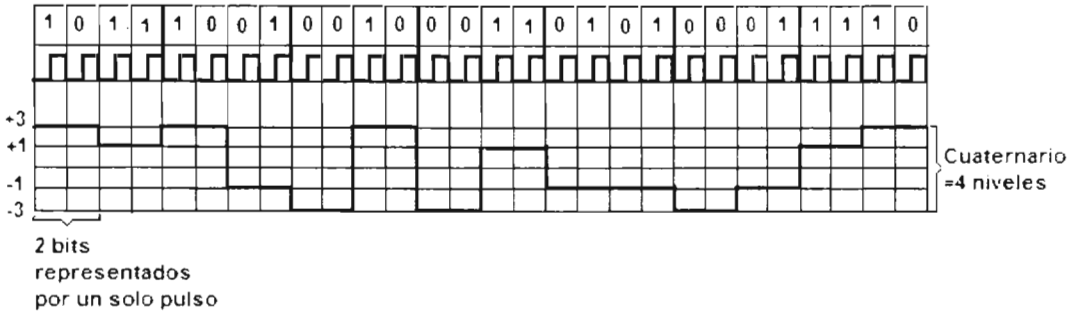


Fig. 1.6.20 Codificación 2B1Q

Existen muchos métodos para codificar datos digitales. Desde él más simple que es el NRZ, el cual se usa en protocolos basados en RS232, pasando por PE que es usado en

ethernet hasta los mas complicados HDB3 que se usan en servicios telefónicos (como la salida de un E1 y la entrada de un E2). La selección de la técnica de codificación esta cargo del diseñador que conoce las restricciones de ancho de banda, sistemas de cableado, velocidad de datos, etc.

Para concluir este tema sobre códigos de línea, resumamos el proceso de codificación entre computadoras, tenemos que en la capa de enlace de datos se prepara la información a transmitir en trenes de bits (0 y 1 lógicos) representados internamente por impulsos de corriente continua. Para su transmisión por los medios de red, el host emisor debe transformar estas señales continuas en señales de corriente alterna, y para ello usa un sistema de codificación, por ejemplo el Manchester es muy usado, creando de esta forma ondas pulsantes basadas en las series de Fourier. Este proceso se lleva a cabo en la tarjeta de red o el modem.

Cuando los trenes de bits han sido convertidos en señales apropiadas, estas son enviadas por los medios físicos hasta el host destino, donde se realiza el proceso inverso, transformándose las señales en sus trenes de bits originales, pudiendo ser procesados por diferentes protocolos de capa, recuperándose así el mensaje original.

1.7 Modulación

La modulación nace de la necesidad de transportar la información a través de un canal de comunicación a la mayor distancia y posible y menor costo. En sistemas digitales, se tiene que realizar una modulación ya que la señal banda base digital tiene problemas para poder ser transmitida por circuitos concebidos como analógicos y que casi siempre son de ancho de banda limitado, como por ejemplo la red pública conmutada que tiene el ancho de banda de la banda vocal, unos 4 Khz., esto aunado a que la señal digital es de baja potencia debido a los bajos voltajes. El canal por el que se transmiten las señales que llevan la información afecta a estas debido a efectos como atenuación, desvanecimiento, ruido blanco aditivo, ruido de fase, interferencia externa, reflexión de señales, refracción, difracción, dispersión.
Debido a estos efectos del canal es que se tiene que usar un sistema de modulación que proteja la calidad de información, que la haga inmune al ruido y evite la interferencia.
La modulación Fig. 1.7.1 es el proceso mediante al cual se utiliza el mensaje o información (sonido, imagen o datos informaticos) como señal moduladora (señal de banda base) para modificar sistemáticamente algún parámetro (amplitud, frecuencia o fase) de una señal portadora de mayor frecuencia, esto produce una señal modulada cuyo ancho de banda esta centrado entorno a la frecuencia de la portadora y así es insertada a un medio de comunicación.

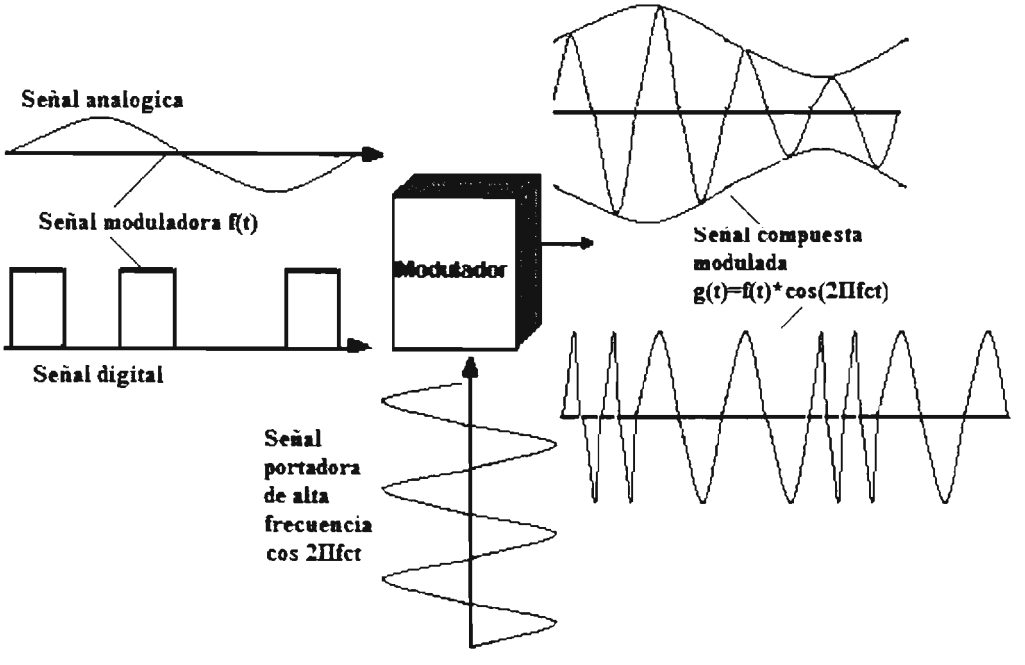


Fig. 1.7.1 Proceso de modulación

Las modificaciones que sufra la señal u onda portadora de las variaciones de la señal moduladora se llama modulación. Dicho proceso de modulación engloba varias técnicas que aplicadas a la onda portadora la harán transportar la información. La información que se transporta puede ser del tipo analógico o digital, de esto se desprende que la modulación se aplica tanto para las comunicaciones analógicas como digitales.
La modulación digital manipula controladamente los parámetros (frecuencia, amplitud o fase) de una onda primaria (portadora) de forma que pueda seguir un patrón de pulsos

(señal digital moduladora) capaz de transportar información de forma correcta. Así la señal modulada viajara a través de la línea de transmisión transportando en forma analógica la información que originalmente se encontraba en forma digital.

Señal en banda base

La señal de banda base es la información misma que se desea transmitir, o sea la señal eléctrica que se obtiene directamente de la fuente de información, esta señal no es siempre adecuada para su transmisión directa a través de un canal, por lo que tienen que ser fuertemente modificadas para facilitar su transmisión Fig. 1.7.2.

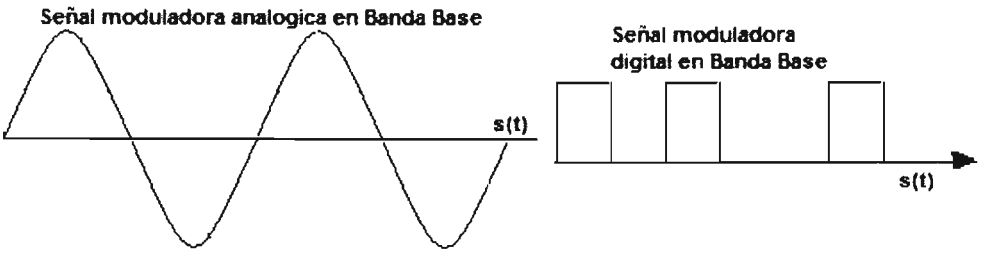


Fig. 1.7.2 Señal moduladora (Banda Base)

Señal Portadora

La señal u onda portadora es una señal continua de tipo senoidal y alta frecuencia f_c, frecuencia que esta centrada en una zona compatible con el medio de transmisión (comparada con la frecuencia de la señal moduladora), Fig.1.7.3, a la cual usualmente se hace variar alguno de sus parámetros (la amplitud, la frecuencia o la fase), esta variación se realiza en proporción a la señal de banda base, al realizarse la variación de alguno de sus parámetros se dice que la onda portadora esta siendo modulada por la señal a transmitir. El papel de la onda portadora en la modulación es bien importante, su importancia la podemos ver cuando se transmiten ondas de radio AM y FM[1], cuando se hace referencia a una estación de radio en el receptor estas se identifican por frecuencias donde esas frecuencias en realidad son las frecuencias de la onda portadora.

Fig.1.7.3 Señal portadora

Las señales portadoras son señales continuas, del análisis de señales estas se representan en la forma:

$P(t)= A\text{sen}(2\Pi f_c t+\varphi)$

Donde:

- A es la amplitud de la portadora en volts
- $w=2\prod f_c$ es la frecuencia angular de la portadora en rad/seg
- φ es el ángulo de la fase de la portadora en radianes

Estos son los parámetros sobre los que se realiza la modulación de la portadora.

Las ondas son perturbaciones mecánicas o electromagnéticas que se propagan a través de un medio y transportan energía. Las ondas electromagnéticas se propagan por el

[1] Estos temas modulación AM, FM se verán en el siguiente tema

espacio sin necesidad de un medio físico. Las ondas mecánicas necesitan un medio (sea sólido, liquido o gaseoso) para poder propagarse, en este caso las partículas del medio oscilan alrededor de un punto fijo sin desplazarse, esto no implica que haya transporte de la materia que constituye al medio. Según el tipo de movimiento que realicen las ondas se clasificaran en:
Ondas longitudinales. Cuando el movimiento de oscilación es paralelo al movimiento de propagación, como el sonido, esto se muestra en la Fig. 1.7.4

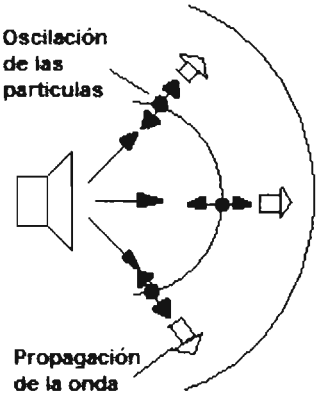


Fig. 1.7.4 Ondas longitudinales

Ondas transversales. Cuando el movimiento de oscilación es perpendicular al movimiento de propagación, como es el caso de las ondas electromagnéticas, este tipo de movimiento se observa con la cuerda de la Fig. 1.7.5

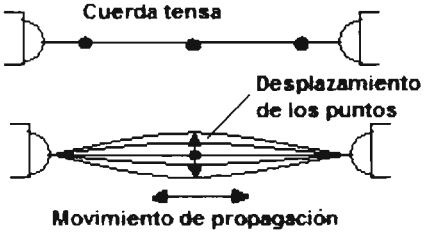


Fig. 1.7.5 Ondas transversales

Las ondas se caracterizan básicamente por su longitud de onda (distancia entre dos puntos que ocupan la misma posición), la frecuencia y la amplitud[2]. El movimiento que realizan las ondas durante su propagación puede tener ciertos fenómenos como son:
Reflexión. La reflexión sucede cuando la onda se encuentra con un nuevo medio que no puede atravesar, entonces cambia de dirección.
Refracción. La onda cambia de dirección cuando pasa de un medio a otro, la velocidad también será distinta.
Difracción. Se da cuando la onda rodea el borde de un obstáculo dejando su trayectoria recta.
Efecto doppler. Este fenómeno se da cuando hay un movimiento relativo entre la fuente emisora de ondas y el receptor de las mismas
La modulación de las señales que entran al sistema de comunicaciones se tiene que realizar ya que no pueden ser enviadas directamente hacia el canal como vienen del transductor, por lo que son modificadas en el proceso de modulación.. Por ello se tiene que modificar la onda portadora para representar el mensaje, la cual tiene propiedades

[2] Características descritas en el tema 1.2 Características de las señales.

que se adaptan mejor al medio de comunicación, la modulación que se realice permitirá tener un control sobre ciertos elementos característicos de la señal portadora.
Las razones por las cuales se realiza la modulación analógica son listadas a continuación:
- Facilita la propagación de la señal de información por cable o por aire.
- Ordena el espectro de radio para distribuir canales a cada información distinta.
- Disminuye las dimensiones de las antenas. Para la radiación eficiente de energía electromagnética las antenas deben tener una dimensión de por lo menos 1/10 de la longitud de onda. Para señales de frecuencias bajas esta dimensión seria muy larga, puesto que la longitud de onda es inversamente proporcional a la frecuencia
$\lambda=c/f$,
donde c es la velocidad de la luz ($3x10^8$ m/s)
Así usando la propiedad de traslación de frecuencias de la modulación las señales se sobreponen a la portadora de alta frecuencia con lo cual se reduce el tamaño de la antena. Es más fácil transmitir una señal de alta frecuencia, además de que su alcance será mayor.
- Optimiza el ancho de banda de cada canal. Cuando se requiere una transmisión en tiempo real, se debe asegurar un adecuado ancho de banda del sistema, si este fuera insuficiente se tendría que disminuir la velocidad de señalización lo que provoca se incremente el tiempo de transmisión. Así si con una señal de banda ancha se modula una portadora de alta frecuencia se reduce el ancho de banda fraccional (ancho de banda absoluto dividido entre la frecuencia central) y con ello se simplifica el diseño de los equipos. Esto lo podemos ver por ejemplo en las señales de TV que tienen un acho de banda de 6MHz se emiten sobre portadoras de frecuencia mucho mayores que en la transmisión de señales de radio AM donde el ancho de banda es de aproximadamente 10 Hz.
- Evita interferencias entre canales. Es posible seccionar y separar una de varias estaciones transmitiendo en un receptor, esto gracias a que cada una tiene asignada una frecuencia portadora diferente. Sin la modulación solo operaria una estación en un área. Dos o más estaciones que transmitan en el mismo medio sin modular producirían una mezcla inútil de señales interfiriéndose entre sí.
- Protege la información de las degradaciones por ruido. Ciertos tipos de modulación tienen la propiedad de suprimir tanto el ruido como la interferencia a costa de requerir un ancho de banda mucho mayor que el de la señal original.
- Define la calidad de la información transmitida
- Modulación para multicanalización. Permite transmitir varias señales sobre un canal de tal manera que cada canal pueda ser captado en el receptor. Por ejemplo realiza 1800 conversaciones telefónicas de una ciudad a otra multicanalizadas y transmitidas sobre un cable coaxial.
- Se modula para superar las limitaciones de los equipos para las frecuencias sobre las que se trabaja, para lo cual la modulación sitúa la señal en la parte del espectro de frecuencias donde las limitaciones de los equipos sean mínimas.

Índice de Modulación
El índice de modulación o porcentaje de modulación mide la intensidad de modulación en una onda portadora y determina la cantidad que varia en amplitud la tensión o corriente de la señal portadora, el cien por ciento es la máxima modulación permitida sin que ocurra distorsión. Este índice describe la cantidad de cambio en amplitud que sufre la portadora producido por la señal de información modulante.

La importancia del índice de modulación radica en la cantidad de potencia que se suministra a las bandas laterales, ya que una señal con portadora muy intensa y con pequeño índice de modulación, proporciona una respuesta más débil en un receptor que una portadora menos intensa con un mayor índice de modulación.
Una portadora será modulada al 50% si su pico positivo de tensión aumenta hasta un valor 50% más grande que el valor máximo de tensión de la portadora sin modular y caerá 50 % en el pico negativo, será modulada al 100% si su pico positivo de tensión alcanza un valor doble del máximo de tensión de la portadora no modulada y cae 100& (cero) en el pico negativo.
Cuando se aplica demasiada amplitud a la señal modulante o de información se produce la sobremodulación, ya que los picos suben a mas del doble del nivel de portadora y bajan mas del doble cayendo a cero permaneciendo en este valor por cierto lapso de tiempo. La señal sobremodulada no es senoidal en el pico negativo por lo que se producen armónicos de la frecuencia moduladora conocidos como distorsión.

1.8 Tipos de modulación

Existen diferentes técnicas de modulación, los tipos de modulación existentes dependerán de la naturaleza de las señales que intervengan en el proceso de modulación y de que parámetro en la señal portadora se modifique para realizar la modulación. Es así como podemos tener los siguiente tipos de modulación:

- Datos analogicos/señales analógicas.
  Representación de la información en forma analógica la cual modula a una portadora analógica, modulación analógica.
- Datos analogicos/señales digitales.
  Representación de la información en forma analógica la cual después de digitalizase se codifica como señal digital. Este tipo de modulación se conoce mas como codificación por pulsos. Este tipo de modulación es el proceso de conversión de analógico a digital[1] para poder transmitir las señales analógicas por un canal digital, lo cual involucra los pasos de muestreo, cuantificación y digitalización para finalmente aplicar la codificación PCM a la señal resultante.
- Datos digitales/señales analógicas.
  Representación de la información en forma digital la cual modula a una portadora analógica, modulación digital.
- Datos digitales/señales digitales.
  Representación de la información en forma digital la cual se codifica en pulsos digitales. Este tipo de modulación realiza el proceso de codificar la información con algún código de línea[2] para su transmisión por el medio digital.

En este tema describiremos brevemente la modulación de señales analógicas por datos analógicos conocida como modulación analógica y la modulación de señales digitales por datos digitales conocida como modulación digital..
Por lo tanto existen básicamente dos tipos de modulación:
Modulación analógica. Realiza el proceso de modulación a partir de señales analógicas de información como la voz, o el audio.
Modulación digital. Realiza el proceso de modulación a partir de señales generadas por fuentes digitales como las computadoras.

Modulación analógica
La modulación analógica se realiza a partir de señales analógicas de información como la voz humana, audio y video en su forma eléctrica.
Una señal analógica no se puede transmitir tal y como es generada por la fuente por varias razones[3], de esas razones dos resaltan que son:
- No es posible transmitir señales en banda base en un medio ambiente libre, por lo que para que la transmisión tenga éxito y cierta calidad será mejor utilizar una señal de frecuencia mayor para su transmisión, que sirva como medio de transporte.
- Se puede realizar una multiplexación en frecuencia gracias a la traslación del espectro en frecuencia lo que permite un mejor aprovechamiento del medio de propagación.

[1] Véase tema 1.5
[2] Véase tema 1.6
[3] Véase tema 1.7

Como sabemos la modulación combina la señal a transmitir x(t) con otra señal llamada portadora p(t) para generar una tercera señal m(t), cuyo espectro de frecuencias estará centrado en torno a la frecuencia fc en la que se quiere situar la señal.
Las técnicas de modulación analógica más conocidas son:
Modulación en amplitud abreviada como AM.
Modulación en frecuencia conocida como FM.
Modulación en fase identificada como PM.

Modulación en amplitud AM

La modulación en amplitud se caracteriza por hacer variar el parámetro amplitud de la señal portadora (señal de alta frecuencia y amplitud constante) en proporción a la amplitud (intensidad) de la información (señal de banda base y baja frecuencia), la variación de la amplitud hace que la distancia entre el punto en que la portadora vale cero y los puntos en que toma el valor máximo y mínimo sea alterada, así la amplitud de la onda portadora variara de acuerdo al valor instantáneo de la señal moduladora. Si la señal moduladora es sinusoidal, la amplitud de la onda modulada variara sinusoidalmente. La señal modulada tendrá una forma similar a la de la señal moduladora en amplitud pero será trasladada a la frecuencia de la señal portadora y de esta manera se sobrepone el contenido de información de la señal moduladora a la señal portadora. La frecuencia de la onda portadora es normalmente miles de hertz mayor que la de la señal moduladora, como se muestra en la Fig. 1.8.1.

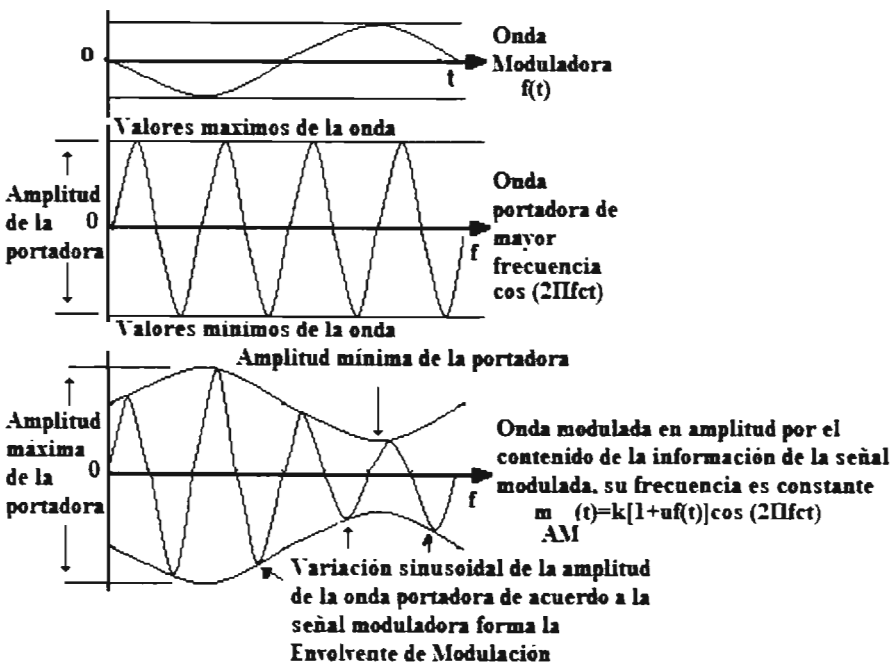


Fig. 1.8.1 Modulación en amplitud

La amplitud de la onda portadora modulada varia entre un valor máximo el cual es mayor que la amplitud de la onda sin modular y un valor mínimo el cual es menor que la amplitud de la onda sin modular. Esto forma una línea exterior a la forma de onda de la portadora lo que se conoce como envolvente de modulación.
Sea f(t) la señal original, la modulación en forma matemática será:
$m_{AM}(t)=k[1+uf(t)][\cos(2\Pi fct)]$
donde : u es el índice de modulación ($0<u<1$).

Frecuencias laterales

Como se puede ver en la Fig. 1.8.1 la amplitud de la información varia la amplitud de la onda portadora. Aparte de esta variación de amplitud al añadir la información con una frecuencia de modulación (f_m) a la portadora se obtienen tres frecuencias, esto es debido a que cada componente de frecuencia de la señal moduladora da lugar a dos frecuencias en la señal modulada, una por encima de la frecuencia portadora y otra por debajo, Fig. 1.8.2.

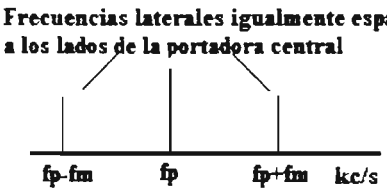


Fig. 1.8.2 Espectro de frecuencias de la modulación AM

Estas frecuencias son:

- La frecuencia de la portadora f_p
- La frecuencia lateral superior que es la suma de las frecuencias de la portadora y de la información (moduladora) f_p+f_m
- La frecuencia lateral inferior que es la diferencia de las frecuencias de la portadora y de la información (moduladora) f_p-f_m

Las dos nuevas frecuencias se llaman las frecuencias laterales superior e inferior y están igualmente separadas a cada lado de la frecuencia de la portadora en una cantidad igual a la frecuencia de la señal moduladora f_m. Esta frecuencia no esta presente en el espectro de frecuencias.

Factor de modulación

El factor de modulación de la onda modulada en amplitud es una relación entre los valores máximos y mínimos de la onda modulada y la amplitud de la señal moduladora, esto se define por la siguiente expresión:

$$m = \frac{\text{Amplitud máx.-Amplitud min.}}{\text{Amplitud máx.+Amplitud Min.}}$$

Si el factor de modulación se expresa como porcentaje se conoce como profundidad de modulación o porcentaje de modulación. Para la modulación sinusoidal el factor de modulación es:

$$m = \frac{Vm}{Vp}$$

Donde:

- Vm es la amplitud de la señal moduladora.
- Vp es la amplitud de la onda portadora.

Debido a este factor de modulación la envolvente de la onda portadora modulada en amplitud varia de acuerdo con la forma de onda de la señal moduladora.

Los dos grandes inconvenientes de la modulación AM son la insuficiente calidad de transmisión y la susceptibilidad a las interferencias ya que debido a que la información se compone de varias ondas dentro de una banda, se necesitaría un gran ancho de banda para transmitir por ejemplo la banda de frecuencias audibles 20-20,000 hz. con buena calidad. Pero como el ancho de banda siempre esta limitado, esta modulación es usada para transmisiones que no requieran gran calidad de sonido o en las que las frecuencias

de información estén próximas entre sí. La modulación AM no provoca demasiado ruido por los desvanecimientos de señal cuando es recibida en el receptor por lo que se puede usar en algunos casos de comunicaciones móviles. Es muy vulnerable a las interferencias producidas por descargas atmosféricas, motores, encendido de automóviles, ya que los ruidos e interferencias alteran muy fácilmente la amplitud de las ondas, puesto que producen señales de radio de amplitud modulada que se captan como ruido en los receptores de AM.
AM es empleada en transmisores de difusión en las bandas larga, media y corta, para la señal de imagen en televisión, radio telefonía de larga distancia, sistemas base-móviles UHF/VHF y para diversos servicios de barcos y aviones.

Modulación en banda lateral única (BLU)
Esta modulación parte de la idea de la modulación AM donde se generan las frecuencias adyacentes a la de la portadora, si la portadora se quiere modular con información que no tiene una frecuencia sino una banda de frecuencias comprendidas entre fm_{min} y fm_{max}, esto es la señal moduladora no es sinusoidal por lo que contiene un cierto numero de frecuencias diferentes, las frecuencias que resultaran de la modulación son:
- Frecuencia de la portadora → fp
- Frecuencia lateral superior producida por fm_{max} → $fp+ fm_{max}$
- Frecuencia lateral inferior producida por fm_{max} → $fp-fm_{max}$
- Frecuencia lateral superior producida por fm_{min} → $fp+ fm_{min}$
- Frecuencia lateral inferior producida por fm_{min} → $fp-fm_{min}$

Toda la gama de frecuencias comprendidas entre $fp+fm_{min}$ a $fp+fm_{max}$ es conocida como banda lateral superior (BLS) y esta compuesta por la banda de frecuencias por encima de la frecuencia portadora.
Toda la gama de frecuencias comprendidas entre $fp-fm_{max}$ a $fp-fm_{min}$ es conocida como bada lateral inferior (BLI) y esta compuesta por la banda de frecuencias por debajo de la frecuencia portadora. Estas bandas de frecuencias se muestran en la Fig. 1.8.3.

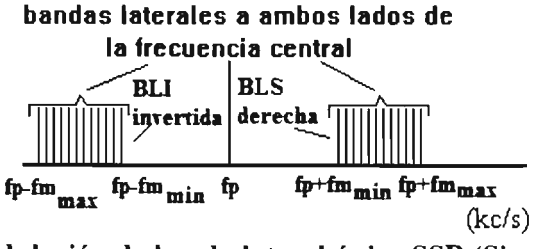


Fig. 1.8.3 Modulación de banda lateral única SSB (Single Side Band)

Por ejemplo sea la frecuencia de la portadora Fp= 1000 Khz
La portadora se quiere modular con información cuyas frecuencias comprenden los 5 y 10 KHz, el espectro resultante será el de la Fig. 1.8.4

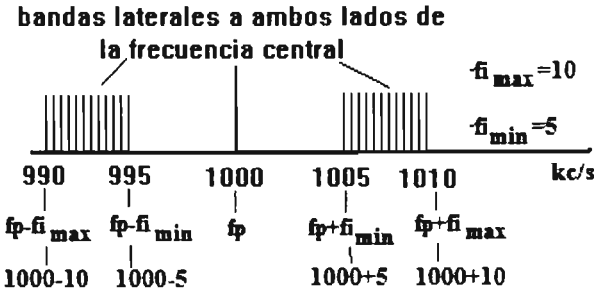


Fig. 1.8.4 Modulación BLU

Si la frecuencia de la portadora es mayor que la moduladora, las bandas laterales son simétricas respecto a la portadora.
La BLI se dice que es invertida por que la frecuencia más alta de esta banda fp- fm_{min} corresponde a la frecuencia más baja fm_{min} de la señal moduladora y al revés. Por su parte la BLS es derecha por que su frecuencia más baja fp+ fm_{min} corresponde a la mas baja de la señal moduladora.
La modulación AM contiene información representada por la señal en ambas bandas laterales (BLI y BLS) por lo que también se conoce como modulación de banda lateral doble (BLD), además, la componente de portadora es de amplitud y frecuencia constantes y no lleva ninguna información
La modulación por banda lateral única (BLU) con supresión de portadora, suprime la portadora y una de las bandas laterales para transmitir la otra banda lateral sin pérdida de información. El receptor reinserta la portadora para poder demodular la señal y transformarla a su forma original, con lo cual se generan algunas ventajas sobre la modulación anteriormente mencionada de portadora continua con ambas bandas laterales (BLD), ventajas como:
- Se obtienen un ahorro en ancho de banda al eliminar una de las bandas laterales y transmitir por ejemplo la banda lateral superior con lo cual se están filtrando las frecuencias de la banda lateral inferior, así comparado con BLD solo requiere la mitad del ancho de banda, las frecuencias de la banda eliminada podrán ser ocupadas por otros canales dentro del espectro de frecuencia del transmisor. Esta modulación se usa en servicios marítimos o aviones, cuando las distancias son grandes y requiere gran potencia de transmisión.
- La relación señal a ruido en el receptor del sistema BLU es mayor que en el de BLD, parte de la mejora se debe al aumento en la relación potencia de banda lateral a potencia total de salida transmitida y el resto es consecuencia de que el ancho de banda necesario se ha reducido a la mitad (la potencia del ruido es proporcional al ancho de banda).
- Un transmisor de BLD produce una potencia de salida (por la portadora transmitida) en todo momento mientras que el transmisor de BLU no, como se suprime la portadora en ausencia de información se ahorra energía de la potencia de corriente continua (cc) tomada de la fuente de alimentación y toda la potencia de transmisión se puede aplicar a una sola banda lateral por eso este sistema se usa mucho en equipos de radioaficionados y servicios de onda corta. El transceptor puede suministrar hasta el doble de potencia que en la modulación AM, además se aumenta la eficiencia total del transmisor.
- Las ondas de radio sufren de la interferencia de desvanecimiento selectivo, con lo que puede haber una considerable distorsión de la señal BLD por que la componente de portadora puede caer por debajo del nivel de las bandas laterales, con lo que las dos

bandas laterales se baten entre sí para producir frecuencias no deseadas, esto no sucede en BLU por que la señal se modula con una portadora de amplitud constante local.
- La supresión de la portadora reduce los niveles de señal que manejan los amplificadores con lo cual se limita el efecto de la no-linealidad y por lo tanto reduce la diafonía. Ya que la no-linealidad en sistemas de telefonía multicanal da lugar a productos de ínter modulación lo que produce diafonía entre canales.
El gran inconveniente de BLU es que los equipos son complejos y caros debido a que se tiene que reintroducir una portadora de la misma frecuencia que la portadora de origen suprimida en el transmisor. La perdida de sincronismo entre las portadoras eliminada y reinsertada producirá desplazamiento en cada componente de frecuencia de la señal demodulada. Por lo tanto la portadora reinsertada debe estar a unos pocos ciclos de la frecuencia de la portadora original.
La modulación BLU es más usada en sistemas de telefonía por radio o líneas de larga distancia.
Este tipo de modulación puede tener tres variantes dependiendo de las bandas que se supriman:
BLS-Banda Lateral superior: Suprime la portadora y la banda lateral inferior.
BLI-Banda lateral inferior: Suprime la portadora y la banda lateral superior.
Banda lateral con portadora suprimida: Solo suprime la portadora.

Modulación en frecuencia FM

La modulación en frecuencia hace variar el parámetro frecuencia de la señal portadora de acuerdo con la intensidad de la onda de información (onda moduladora). La amplitud y la fase de la onda modulada serán constantes e igual que la de la onda portadora, la frecuencia cambia en función de los cambios de amplitud y frecuencia de la señal a transmitir, Fig. 1.8.5.

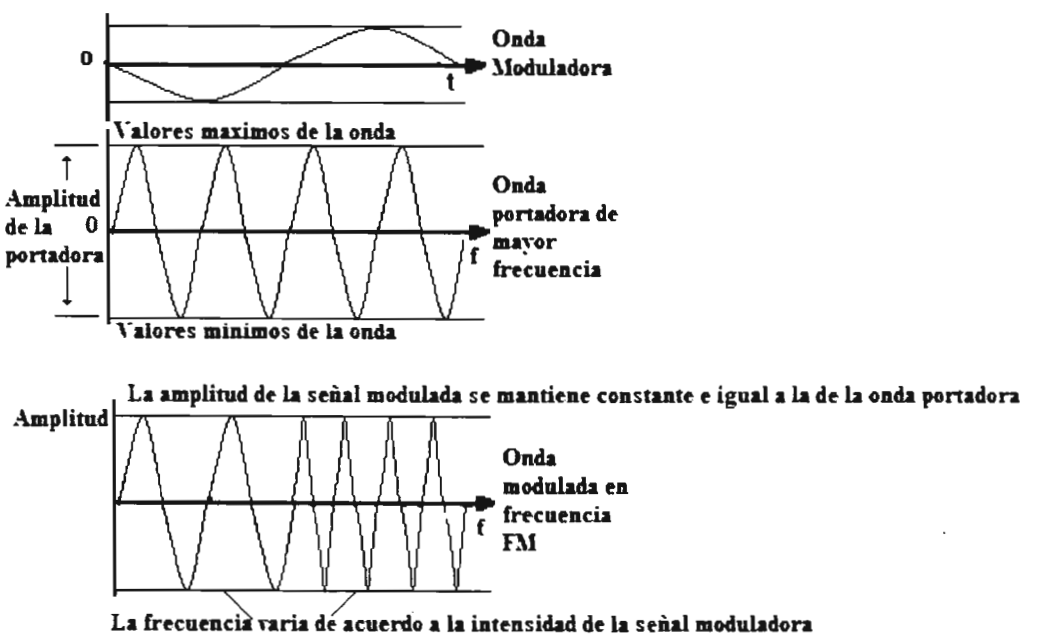


Fig. 1.8.5 Modulación en frecuencia FM

La frecuencia de la onda portadora oscila mas o menos rápidamente según la onda moduladora, por ejemplo si se aplica una moduladora de 100 hz. la onda modulada se

desplaza arriba y abajo cien veces en un segundo respecto de su frecuencia central que es la portadora. El grado de variación dependerá del volumen con que se module la portadora conocido como índice de modulación. Matemáticamente se representa de la siguiente forma:

$m(t)=\cos(2\Pi fct+\Phi(t))$

Donde: $\Phi(t) = n_f * x(t)$ n_f es el índice de modulación en frecuencia.

En este tipo de modulación tenemos un parámetro importante que es la frecuencia instantánea:

$F_i(t)=fc+(1/2\Pi)\ \Phi'(t)$

El ruido e interferencias no afectan a la modulación en FM ya que estos afectan a la amplitud, y la información va en las variaciones de frecuencia, no en la amplitud que se mantiene constante.

Las principales características de FM son:

- Su modulación y su propagación es por ondas directas como consecuencia de su ubicación en la banda de frecuencias de VHF.
- La relación señal a ruido es mayor en el receptor de FM que en el de AM BDL.
- La amplitud de una onda modulada FM es constante lo que permite construir transmisores de mayor eficiencia.
- El receptor de FM al aplicar el efecto de captura puede suprimir la más débil de dos señales que se reciben simultáneamente en o cerca de la misma frecuencia.
- Posee una gama dinámica de amplitudes de la señal moduladora que puede transmitir.

El uso típico de la modulación FM es en la radiodifusión de FM

En la modulación FM la calidad del sonido, imagen o alta fidelidad es mayor que en AM o SSB, esta calidad se debe a que la FM tiene gran robustez ante fenómenos de desvanecimiento de la señal recibida ya que crea un conjunto de complejas bandas laterales cuya extensión depende de la amplitud de la onda moduladora, al incrementarse las bandas laterales la anchura del canal FM será más grande que el tradicional de onda media y por lo tanto también será mayor la anchura de banda de sintonización de los receptores. Además como no se altera la frecuencia portadora, señales sonoras o información de otro tipo como datos comprenden un mayor abanico de frecuencias moduladoras sin que esto requiera mayor ancho de banda, por esto es muy usada en estaciones de radiodifusión musical. FM también se usa en telefonía móvil, televisión y servicios de comunicación entre empresas.

El mayor ancho de canal de FM no se debe a la tecnología (aunque si requiere un mayor consumo de espectro) sino debido a que la banda de MF (radio) se encontraba saturada a FM se le adjudico la banda de VHF, espectro con grandes posibilidades para radiodifusión, TV y alta fidelidad, por lo que sus canales tienen una capacidad muy superior a sus necesidades, normalmente la anchura de sus canales es de entre 100 y 200 Khz.

La propagación de la banda de VHF se realiza con ondas directas o espaciales que se caracterizan por su direccionalidad y limitada cobertura ya que por ser direccionales se pierden en el espacio al ser absorbidas o apagadas por los obstáculos. VHF tiene un índice de refracción mayor al de las bandas superiores por lo que puede alcanzar mayores coberturas usando la refracción troposferica, pero su cobertura de propagación es menor a la de AM por la direccionalidad de las ondas directas o espaciales, esta cobertura reducida también la hace ser usada para servicio local. Las antenas para FM son de pequeñas dimensiones y polarización horizontal por su pequeña longitud de onda. También usa antenas de polarización circular para radiar en los planos horizontal y vertical para poder ser recibidas en antenas de automóvil.

FM es muy empleado para la difusión de sonido en VHF, para las señales del sonido de televisión en UHF, para algunos sistemas móviles-base, para algunos servicios de barcos y aviación y para sistemas de radiotelefonía de banda ancha.
El gran inconveniente de FM es el mayor ancho de banda requerido que AM, sin embargo esto también lo hace más resistente a las interferencias.

Multiplexión por división de frecuencia
La multiplexión es un conjunto de técnicas que permiten la transmisión simultanea de múltiples señales o canales a través de un único enlace.
La multiplexión por división de frecuencias es aplicada generalmente para señales analógicas. La multiplexión se aplica cuando el ancho de banda del enlace es mayor que los anchos de banda combinados de las señales a transmitir. Para poder realizar esta multiplexación se utilizan diferentes portadoras con distintas frecuencias para transmitir (estas frecuencias no deben interferir con las frecuencias de los datos originales a transmitir), para evitar la interferencia entre los canales se usan bandas de seguridad, Fig. 1.8.6.

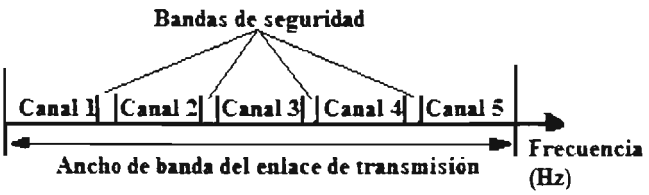


Fig. 1.8.6 Multiplexión por división de frecuencia

La multiplexión por división de frecuencia traslada la frecuencia de un canal a una posición más alta en el espectro de frecuencias. La parte concreta del espectro de frecuencia a la que se desplaza el canal se determina por la frecuencia de la onda portadora sinusoidal que se modula. Para aclarar el funcionamiento de múltiplexión por división de frecuencia, considérese el caso de transmitir tres canales telefónicos de ancho de banda de 300 a 3400 hz. por una línea común. El primer canal será transmitido directamente por la línea y ocupara el ancho de banda de 300 a 3400 Hz. El segundo y el tercero ya no se puede transmitir directamente ya que no se podría separar el primer canal de los otros. Para esto a los dos canales se les hace una translación o desplazamiento de frecuencia, siendo entonces las bandas de frecuencia de 4300 a 7400 hz. y de 8300 a 11400 hz., antes de ser transmitidas por la línea. Ahora ya se puede transmitir por la línea común ya que entre ellos hay una separación de 900 hz. por lo que no habrá interferencia entre canales. En la recepción se separan los tres canales y se restituirán el segundo y tercer canales a sus bandas de frecuencias originales, este proceso de multiplexación por división de frecuencia se puede implementar con un circuito como muestra la Fig. 1.8.7.. El ancho de banda del circuito común debe ser 300 a 11400 Hz., la línea puede ser un cable telefónico, radio enlace UHF/VHF o microondas,

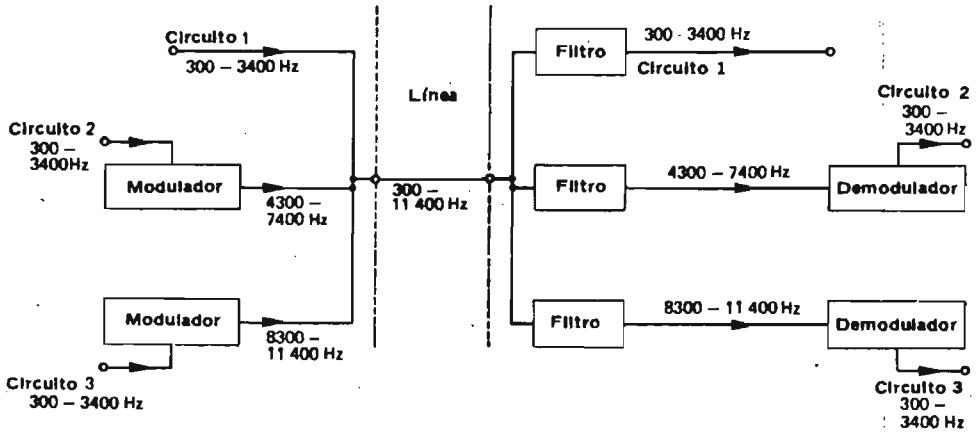


Fig. 12.1.– Sistema sencillo de 3 canales en múltiplex por división de frecuencias.

Fig.1.8.7 Sistema sencillo de multiplexación por división de frecuencias.

Esta traslación es empleada en la radiodifusión y televisión, ya que las antenas que reciben la radiodifusión funcionan con audio frecuencias por lo que antes de la transmisión la parte de audiofrecuencia se desplaza a un punto mas alto en el espectro de frecuencias en el que las antenas pueden funcionar con eficiencia.
Para que las estaciones de radiodifusión estén separadas entre sí en el espectro de frecuencias las emisiones de radio son trasladas en frecuencia a bandas propias determinadas según acuerdos.

Modulación en fase PM
Esa modulación manipula la variación de la fase de la señal portadora según la señal de información de entrada, se representa matemáticamente como:
$m(t)=\cos(2\Pi fct+\Phi(t))$
Donde : $\Phi(t) = n_p * x(t)$ n_p es el índice de modulación en fase.

Modulación digital
La modulación digital usa señales generadas por fuentes digitales como la computadora (DTE) para modular la portadora, en este proceso la fuente de datos es digital y el medio de transmisión es analógico, un ejemplo de este proceso es la transmisión de datos digitales desde una computadora a través de la línea telefónica empleando normalmente un modem. En la modulación digital tenemos los siguientes tipos de modulación, cada una afectando parámetros característicos de la señal analógica portadora:
- Modulación ASK. Afecta la amplitud de la señal analógica.
- Modulación FSK. Afecta la frecuencia de la señal analógica.
- Modulación PSK. Afecta a la fase.
- Modulación QAM. Afecta a la fase y la amplitud.

Modulación ASK
Esta técnica de modulación por desplazamiento en amplitud ASK (Amplitude Shift Keying) hace variar la amplitud de la onda portadora entre dos valores según la cadencia de la señal digital para transmitir de esta manera la información, Fig. 1.8.8.

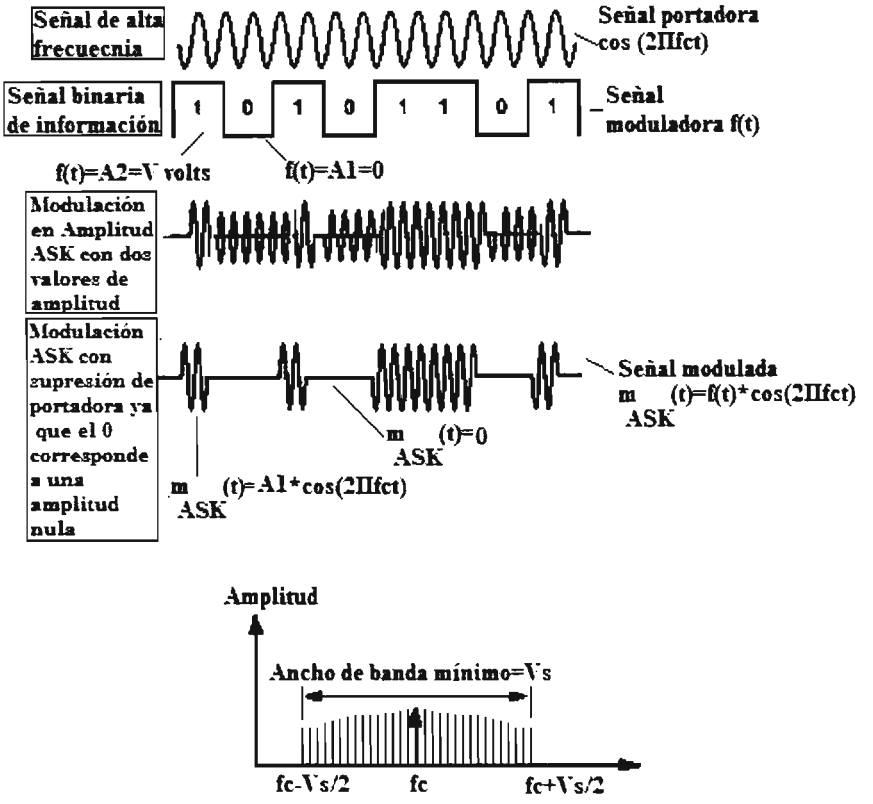


Fig.1.8.8 Modulación ASK

Este tipo de modulación es muy sensible a la amplitud y presenta problemas de distorsión y potencia, es muy sensible a interferencias de ruido eléctrico que puede provocar errores en los datos recibidos, no es un sistema de modulación muy eficaz, normalmente se emplea en conjunción con la modulación en fase, lo cual hace más eficaz el proceso de modulación.. La señal modulada representara al 1 binario con una onda sinusoidal de amplitud A, mientras el 0 se representa con una amplitud menor que A. Los parámetros de frecuencia y fase permanecen sin alteración.

Se usa normalmente en fibras ópticas, donde un led emite mucha luz o poca para representar los pulsos. Si hay un pulso es que se esta mandando un 1 si no lo hay se esta mandando un 0. La señal a transmitir será:

La señal digital a transmitir es f(t) esta señal representa la información con dos niveles de tensión A_1=0 V y A_2 = V volts.

La señal portadora de alta frecuencia será del tipo senoidal $\cos(2\Pi f_c t)$

La señal modulada en amplitud ASK será: $m_{ASK}=f(t)^* \cos(2\Pi f_c t)$. Este producto de las funciones produce el corrimiento del espectro de frecuencia de la señal original f(t) hasta la frecuencia f_c de la señal portadora. Así:

- Para el Cero binario $f(t)= A_1=0$ V, por lo tanto
  $m_{ASK}(t)= A_1 \cos(2\Pi f_c t) =0$
- Para el Uno binario $f(t)=A_2$ por lo tanto
  $m_{ASK}(t)= A_2 \cos(2\Pi f_c t)$

Dependiendo del valor dado a la amplitud se transmitirá uno u otro símbolo.

De la Fig. 1.8.8 podemos ver que el ancho de banda mínimo será Vs ya que

$AB_{ASK}=(1+r)^*Vs$

Donde:

- Vs es la velocidad en símbolos o tasa de baudios

- r es un factor de filtrado de línea y toma los valores de $1 \leq r \leq 0$

Asimismo el ancho de banda máximo será el doble de Vs. En general en la modulación ASK el ancho de banda de la señal modulada será el doble de la señal original debido al corrimiento de frecuencia que sufre la señal hacia la frecuencia portadora:
$AB_{ASK}=2AB_{f(t)}=V_{baudios}=V_{bps}$
Donde V_{bps} es la velocidad de entrada (bps) de los bits de la señal digital que se va a modular.
Esto se deriva de la formula de velocidad de Nyquist:
$V_{baudios}=2AB_{f(t)}$
Y como en ASK un símbolo transporta un solo bit:
$V_{baudios}=V_{bps}$
La modulación ASK normalmente no se usa en la construcción de modems ya que no permiten implementar técnicas que permitan elevar la velocidad de transmisión.

Modulación FSK
La modulación por desplazamiento de frecuencia FSK (frecquency Shift keying) binaria, Fig. 1.8.9 es una forma de modulación angular de amplitud constante similar a la FM convencional, excepto que la señal modulante es un flujo de pulsos binarios que varia entre dos niveles de voltaje discreto en lugar de una forma de onda analógica que varia continuamente.

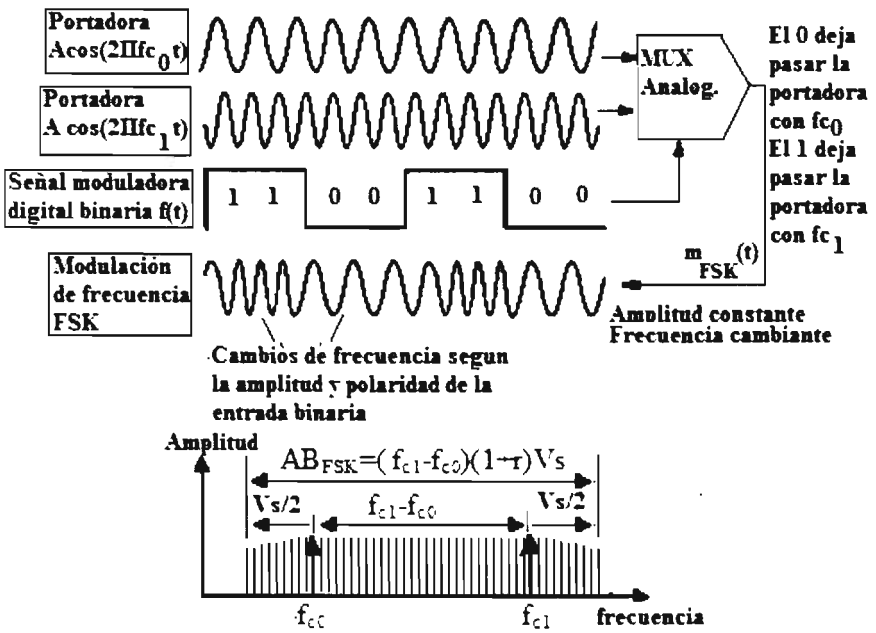


Fig. 1.8.9 Modulación FSK

Esta técnica modifica la frecuencia de la señal portadora según la señal digital que se transmite, esto es, asigna una frecuencia diferente a cada estado significativo de la señal digital. En la señal modulada la frecuencia mas alta representara al 1 binario y el 0 binario se representara con una frecuencia diferente. Dos valores típicos de las portadoras usados son 1.4 y 2.2 Khz, valores que se encuentran dentro de la banda audible de voz. Se usa en las comunicaciones asíncronas sin referencia de reloj debido a que se tienen que detectar las diferencias de frecuencia.

La expresión general para la señal FSK binaria es

$$v(t)=V_c\cos[(w_c+\frac{v_m(t)\,\Delta w}{2})t]$$

Donde :

- v(t) es la forma de onda binaria FSK
- V_c es la amplitud pico de la portadora no modulada
- w_c es la frecuencia de la portadora en radianes
- $v_m(t)$ es la señal modulante digital binaria
- Δw es el cambio de frecuencia de la salida en radianes

Para realizar la modulación FSK se parte de una señal de entrada conteniendo la información en forma digital binaria con valores 0 y 1.

Se tendrán dos portadoras con diferente frecuencia y la misma amplitud A ($A\cos(2\Pi f_{c0}t)$ y $A\cos(2\Pi f_{c1}t)$).

Los dos valores binarios se representaran en la señal modulada por dos frecuencias diferentes f_1 y f_2 muy próximas a la portadora:

Cuando llega un cero binario la salida del modulador es $m(t)=A\cos(2\Pi f_{c0}t)$ f_{c0}=frecuencia de la portadora para el 0 binario.

Cuando llega un uno binario la salida del modulador es $m(t)=A\cos(2\Pi f_{c1}t)$ f_{c1}=frecuencia de la portadora para el 1 binario.

Donde f_{c0} y f_{c1} son desplazamientos de frecuencia de igual magnitud pero en sentidos opuestos alrededor de la portadora.

La señal modulada tomara alguna de las dos frecuencias diferentes cuando al entrar las dos portadoras a un multiplexor se dejara pasar una o la otra según sea el dato un 0 ó 1.

El ancho de banda será:

$$AB_{FSK}=(f_{c1}-f_{c0})(1+r)Vs$$

Donde:

- Vs es la velocidad en símbolos o tasa de baudios
- r es un factor de filtrado de línea y toma los valores de $1\leq r\leq 0$

En función del índice de modulación:

$$AB_{FSK}=2AB_f(1+\beta)$$

Donde:

- $\beta=\Delta f/AB_f$ es el índice de modulación
- AB_f es el ancho de banda de la señal original de información.

El ancho de banda mínimo será:

$$AB_{FSK}=2AB_f$$

De la ecuación que es la expresión general de la señal FSK binaria podemos ver que la amplitud de la portadora V_c se mantiene constante con la modulación y la frecuencia de la portadora de salida w_c cambia por una cantidad igual a $\pm\,\Delta w/2$. El cambio de frecuencia $\Delta w/2$ es proporcional a la amplitud y polaridad de la señal de entrada binaria. De esta manera si el uno binario es +1V y el cero -1V se producen cambios de frecuencia de $+\Delta w/2$ y $-\Delta w/2$.

La rapidez de cambio de la frecuencia de la portadora será igual a la rapidez de cambo de la señal de entrada binaria $v_m(t)$ (o sea la razón de los bits de entrada). Así la frecuencia de la portadora de salida cambia entre $w_c+\Delta w/2$ y $w_c-\Delta w/2$ a una velocidad igual a f_m (frecuencia de la señal moduladora).

La modulación FSK (transmisión por desplazamiento de frecuencia) deriva su nombre del comportamiento que tiene la frecuencia portadora durante la modulación, ya que la frecuencia central o portadora se desplaza (se desvía) por los datos de la entrada binaria. Este desplazamiento es de la siguiente manera, conforme cambia la señal de entrada

binaria de 0 lógico a 1 lógico y viceversa, la salida del FSK se desplaza entre dos frecuencias; una frecuenta de marca o de 1 lógico y una frecuencia de espacio o de 0 lógico. Así hay un cambio en la frecuencia de salida cada vez que la condición lógica de la señal de entrada binaria cambia, por lo tanto la razón de salida del cambio es igual a la razón de entrada del cambio.
En modulación la digital la razón (rapidez) de cambio en la entrada del modulador se llama razón (tasa) de bit (bit-rate) y tiene como unidades los bits por segundo (bps).
La rapidez (razón) de cambio a la salida del modulador se conoce como baudio o razón de baudio (baud-rate) y es igual al reciproco del tiempo de un elemento de señalización de salida. El baudio es la razón de línea en símbolos por segundo.
En FSK como las razones de cambio de entrada y salida son iguales (bit rate=baud rate) por lo tanto la razón de bits y de baudios son iguales.
La modulación FSK puede ser del tipo coherente, en la cual se mantiene la fase de la señal cuando se asigna la frecuencia. En FSK no coherente la fase no se mantiene al momento de asignar la frecuencia, esta se da cuando se usan dos osciladores independientes para la generación de frecuentas distintas.
FSK es menos sensible a errores que ASK. Normalmente se usa en radio en el intervalo entre los 3 y 30 MHz, para mayores velocidades de transmisión que ASK, para transmisiones de teléfono a altas frecuencias y para redes Lan con cables coaxiales.
FSK se usa en módems para velocidades de hasta 2400 baudios.

Modulación PSK

La modulación por desplazamiento de fase PSK (Phase Shift Keying) también conocida como BPSK representa con dos desplazamientos en la fase de la señal portadora analógica los dos estados binarios de la señal de banda base, un 0 se representa como una señal con igual fase que la señal anterior y un 1 con fase opuesta a la anteriormente enviada. La variación de la fase se realiza con relación a una fase de referencia de 180° para representar el paso de un 0 a un 1, Fig. 1.8.10.

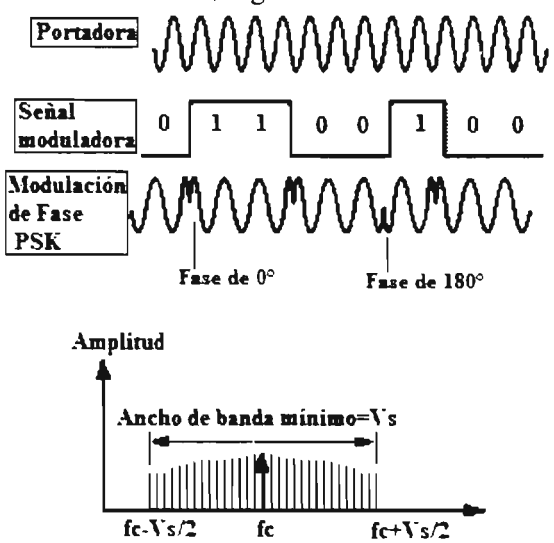


Fig. 1.8.10 Modulación PSK

Al igual que en las modulaciones ASK y FSK las fases no son elegidas arbitrariamente, sino que son determinados por la ITU para maximizar a posibilidad de leer el dato recibido con la mayor probabilidad de no cometer un error.
- Cero binario $A\cos(2\pi f_c t)$
- Uno binario $A\cos(2\pi f_c t + \Pi)$

Cuando la entrada es un 0 lógico, la fase absoluta de salida de PSK es 180°. Si la entrada es un 1 lógico entonces la fase de salida es 0°.
$AB_{PSK}=(1+r)*Vs$
Donde:

- Vs es la velocidad en símbolos o tasa de baudios
- r es un factor de filtrado de línea y toma los valores de $1 \leq r \leq 0$

La fase que se suma en PSK será diferente en función del símbolo que se quiera transmitir.

El ancho de banda mínimo para transmitir una señal modulada PSK es:
$AB_{PSK}=2AB_f=V_{baudios}=V_{bps}$
Como usa 1 bit por cada símbolo, tenemos:
Si Vs=2400 baudios, la V_{bps}=2400 bps

Modulación Diferencial de Fase DPSK
La modulación diferencial de fase DPSK (Diferencial Phase Shift Keying) es una variante de PSK, la cual no trabaja con fases absolutas sino con cambios de fase en la señal de salida, así cuando se transmite un 1 lógico no se produce cambio de fase en la señal analógica de salida y cuando se transmite un 0 lógico la señal de salida producirá un cambio de fase de +180° la cual toma el ángulo de fase del intervalo anterior como referencia para desplazar la fase en + o en -90° en relación con el bit anterior para representar al digito binario.

Representación de la modulación PSK
La modulación PSK se puede representar en dos formas con un diagrama vectorial en el que se representa la amplitud y la fase de los símbolos que representan a los bits y con un diagrama o constelación de puntos, Fig. 1.8.11

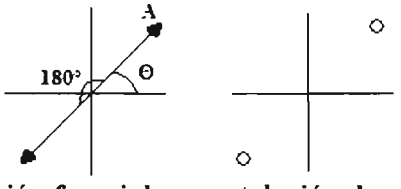


Fig. 1.8.11 Representación fasorial y constelación de puntos de modulaciones multinivel

De la Fig. 1.8.11 vemos que la representación fasorial usa un vector cuyo modulo indica la amplitud A y el ángulo Θ=45° indica la fase y por lo tanto indirectamente la frecuencia (la frecuencia esta en función del ángulo), entonces se usa un vector para representar un 1 binario y un vector opuesto 180° para el 0 binario. Conforme aumentan las fases las representaciones fasoriales se complican por lo que es más fácil representar los estados modulados como puntos en un plano polar que analizar la grafica en función del tiempo en un plano coordenado, estas graficas vectoriales son más legibles sin el vector, entendiéndose que la distancia al origen es la amplitud de la señal. Estas graficas se conocen como diagramas de constelación de puntos. Esto se extiende para representar m fases.

Los métodos de modulación digital nativos ASK, FSK y PSK no son muy eficientes en términos del ancho de banda utilizado. Estos solo pueden transmitir una de dos señales durante cada intervalo de señalización. Estos métodos tienen una eficiencia teórica de

ancho de banda de 1 bps/Hz, pero para manejar mayores velocidades de comunicación se requiere transmitir mas bits por segundo, lo cual ha conducido a la modulación de múltiples fases o M-aria..

Modulaciones PSK en múltiples fases (MPSK) o n-arias.

Dentro de la modulación PSK tenemos muchas variantes dependiendo del numero de fases usadas para realizar la modulación por lo cual a este tipo de modulación también se le conoce como modulación en multiples fases MPSK.
La señal PSK tiene dos posibles fases de salida (fases absolutas).
MPSK tiene n fases posibles para una misma frecuencia portadora, así si la modulación tiene mas de dos valores posibles n>2 (n-aria) modifica la fase en los n valores posibles, esto es, usando varios ángulos de fase, uno por cada tipo de señal, se pueden codificar mas bits con iguales elementos de señal:
$M=2^n$
Donde:

- n es el numero de bits.
- M es él numero de combinaciones posibles con n bits.

La formula nos dice que se pueden convertir grupos de n bits de información en una señal analógica de amplitud constante y con 2^n fases posibles.
Se puede ampliar a un numero cualquiera de bits; por ejemplo usando 8 fases se pueden transmitir tres bits cada vez. Además cada ángulo puede tener varias amplitudes por lo que un modem de 9600 bps puede utilizar PSK de 12 ángulos con 2 posibles amplitudes.
En estos tipos de modulaciones la velocidad en bps se calcula con la siguiente relación entre la tasa de baudios y la tasa de bits:
$V_{bps}=nVs$
Y el ancho de banda es:
$AB=Vs(1+r)/n$
Donde:

- n=numero de bits por cada símbolo.
- Vs es la velocidad en símbolos o tasa de baudios.
- r es el factor de filtrado de línea $1 \leq r \leq 0$

Modulación QPSK
La modulación QPSK (Quadrature phase-shift keying), forma parte de los tipos de modulación MPSK. En este modulador entra una señal binaria de información con niveles de tensión de ±1 V y usa una señal portadora cos $2\Pi f_c t$.
QPSK divide el tren de datos a transmitir en pares de bits consecutivos llamados dibits, codificando cada bit como un cambio de fase con respecto al elemento de señal anterior. Usa 2 bits por cada símbolo, así n=2 y M=4, por lo tanto tenemos una modulación de 4 estados de fases diferentes para la transmisión de los bits. La salida del modulador será la señal portadora con 4 fases posibles a la misma frecuencia f_c y amplitud constante.
En QPSK de los datos de entrada binaria que se componen por grupos de 2 bits llamados dibits (Q, I) y que producen cuatro posibles combinaciones de bits 00, 10, 01 y 11, de cada par de bits entra un bit a un modulador, en los moduladores se aplica la ortogonalidad de senos y cosenos para transmitir dos señales diferentes simultáneamente en la misma frecuencia de portadora, así en cada modulador se mezclan con la frecuencia de la portadora la cual en uno de ellos entra desfasada 90° y a la salida del modulador se mezclan dos senoidales ($\pm\cos 2\Pi f_c t$ y $\pm\text{sen } 2\Pi f_c t$) con

signos dependientes de la polaridad del bit de entrada. Así dependiendo de los datos que se transmitan se generara un desfase u otro ya que las combinaciones de bits se hacen corresponder a los ángulos de los cuadrantes del sistema cartesiano:
11 → p=45°
01 → p=135°
00 → p=225°
10 → p=315°
La tabla 1.8.1 nos muestra estos valores.

Entrada Binaria (Dibits)		Señal de salida QPSK $F_{QPSK}(t)$	Fase de salida de la señal QPSK
Q	I		
0	0	$-\cos 2\Pi f_c t - \text{sen } 2\Pi f_c t$	-135°
0	1	$-\cos 2\Pi f_c t + \text{sen } 2\Pi f_c t$	-45°
1	0	$+\cos 2\Pi f_c t - \text{sen } 2\Pi f_c t$	+135°
1	1	$+\cos 2\Pi f_c t + \text{sen } 2\Pi f_c t$	+45°

Tabla 1.8.1 Tabla de valores de las fases de la modulación QPSK

QPSK formara un diagrama fasorial y un diagrama de constelación de puntos Fig. 1.8.12 con cuatro elementos cada uno representando 2 bits.

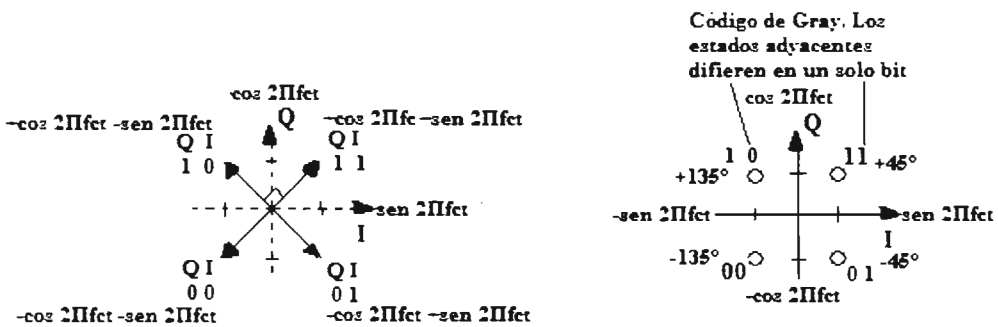


Fig. 1.8.12 Diagrama de fasores de la modulación QPSK y constelación de puntos

Así en QPSK se tienen 4 desplazamientos de 45°, 135°, 225° o 315° para representar respectivamente al 11, 01, 00 y 10.
La separación angular entre fases de salida adyacentes es de 90° y cada dibit difiere del adyacente en un bit. Este sistema de codificación es conocido como código Gray.
Si Vs=2400 baudios, la V_{bps}=4800 bps
QPSK tiene una mejor eficiencia espectral (relación entre la velocidad de información en bps y el ancho de banda necesario en hz.). Por lo tanto requiere menor ancho de banda para transmitir la misma información debido a que cada nivel de fase lleva 2 bits de información.

Modulación 8PSK
La modulación 8PSK (Eight-phase PSK), forma parte de los tipos de modulación digital MPSK. En este modulador entra una señal binaria de información con niveles de tensión de ±1 V y usa una señal portadora $\cos 2\Pi f_c t$
En 8PSK M=8 y por lo tanto n=3 ($M=2^3$), usa 3 bits por cada símbolo, por lo tanto tenemos una modulación de 8 estados de fases diferentes para la transmisión de los bits.

Así la salida del modulador será la señal portadora con 8 fases posibles a la misma frecuencia f_c y amplitud constante.
En 8PSK los datos de entrada binaria se componen por grupos de 3 bits (tribits Q, I, C) que producen ocho posibles combinaciones de bits. De cada tres bits entra un bit I a un convertidor D/A junto con el C, mientras el bit Q entra a otro convertidor D/A junto con C invertido, de cada convertidor se obtienen de las 2 entradas digitales una señal PAM de 4 niveles tensión. Fig. 1.8.13

I C	Señal PAM Canal I-C
0 0	-0.541 V
0 1	-1.307 V
1 0	+0.541 V
1 1	+1.307 V

Q $\bar{C}$	Señal PAM Canal Q-$\bar{C}$
0 1	-1.307 V
0 0	-0.541 V
1 1	+1.307 V
1 0	+0.541 V

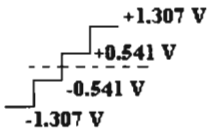


Fig. 1.8.13 Convertidores A/D I-C y $\bar{Q}$-C. Señal PAM generada de cada uno.

Las 2 señales PAM entran cada una a un modulador balanceado y se mezclan con la frecuencia de la portadora la cual en uno de ellos entra desfasada 90° (con Q-C* cos $2\pi fct$)) y así a las salidas de los moduladores se suman linealmente para dar la señal 8PSK. Los posibles valores de la señal 8PSK se muestran en la tabla 1.8.2.

Entrada binaria (Tribits)			Señal de salida 8PSK $f_{8PSK}(t)$	Fase de salida de la señal 8PSK
Q	I	C		
0	0	0	-1.307cos w_ct-0.541sen w_ct	-112.5°
0	0	1	-0.541cos w_ct-1.307sen w_ct	-157.5°
0	1	0	-1.307cos w_ct+0.541sen w_ct	-67.5°
0	1	1	-0.541cos w_ct+1.307sen w_ct	-22.5°
1	0	0	+1.307cos w_ct-0.541sen w_ct	+112.5°
1	0	1	+0.541cos w_ct-1.307sen w_ct	+157.5°
1	1	0	+1.307cos w_ct+0.541sen w_ct	+67.5°
1	1	1	+0.541cos w_ct+1.307sen w_ct	+22.5°

Tabla 1.8.2 Tabla de los valores de modulación en fase 8PSK

La Fig.1.8.14 muestra el diagrama de fasores y la constelación de puntos para la modulación 8PSK.

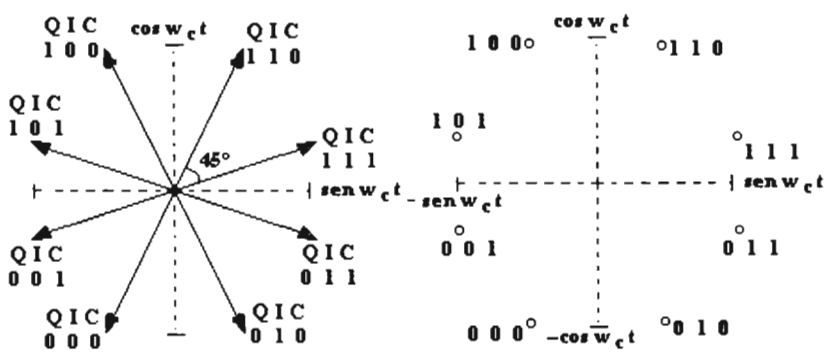


Fig. 1.8.14 Modulación 8PSK, diagrama de fasores y constelación de puntos

Se puede observar en la Fig. 1.8.13 que la amplitud de la señal es constante, cada tribit difiere del adyacente en un bit (Código Gray) y las separaciones entre fasores adyacentes son de 45°, el ángulo de separación entre fasores ha disminuido para 8PSK comparado con QPSK.
En 8PSK si Vs=2400 baudios, la V_{bps}=7200 bps

Modulación 16PSK
La modulación de 16 fases PSK (Sixteen.phase PSK), usa 4 bits por cada símbolo por lo que consiste en 16 estados de fase distribuidos en una circunferencia con igual amplitud. Así M=16 por lo que n=4 bits conocidos como quadbits. Su amplitud seguirá siendo constante. Sus valores se muestran en la tabla 1.8.3.

Renglón	Señal binaria (Quadbits)				Fase de salida	Renglón	Señal binaria (Quadbits)				Fase de Salida
1	0	0	0	0	11.25°	9	1	0	0	0	191.25°
2	0	0	0	1	33.75°	10	1	0	0	1	213.75°
3	0	0	1	0	56.25°	11	1	0	1	0	236.25°
4	0	0	1	1	78.75°	12	1	0	1	1	258.75°
5	0	1	0	0	101.25°	13	1	1	0	0	281.25°
6	0	1	0	1	123.75°	14	1	1	0	1	303.75°
7	0	1	1	0	146.25°	15	1	1	1	0	326.25°
8	0	1	1	1	178.75°	16	1	1	1	1	348.75°

Tabla 1.8.3. Tabla de valores de la modulación 16PSK

De los valores de la tabla 1.8.3 se observa que la separación angular entre fasores adyacentes es de solo 22.5°. En la Fig. 1.8.15 tenemos la constelación de puntos de 16PSK.

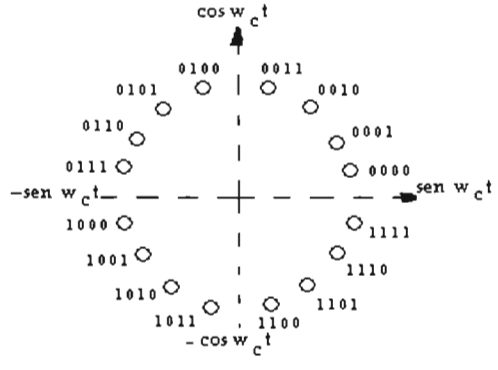


Fig. 1.8.15 Constelación 16PSK

Con 16PSK tenemos que si Vs=2400 baudios, la V_{bps}=9600 bps.
En 16PSK las fases se encuentran muy cercanas con lo que el error o ruido permitido es mínimo ya que se corre el riesgo de que se confundan o traslapen estas fases.
16PSK se usa en sistemas de baja y media capacidad, hasta 34 Mbps.

Consideraciones respecto a la modulación MSPK.
El ancho de banda mínimo para transmitir una señal digital MPSK es:
$B_{MPSK}=2B_F$
Donde B_F es el ancho de banda de la señal digital de información f(t).

La relación entre la velocidad de transmisión en baudios (símbolos/seg) y el ancho de banda de la señal digital, según la velocidad de Nysquist es:
$V_B=2B_F$
Ya que en un símbolo se transmiten k bits de información:
$V_b=kV_B$
Donde V_b es la velocidad de transmisión en bps.
El ancho de banda mínimo en función de la velocidad de bps es:
$B_{MPSK}=V_b/k$
Por lo tanto en MPSK el ancho de banda mínimo para transmitir una señal MPSK es igual a la velocidad en bps a la entrada del modulador dividido por el numero de bits transmitidos por símbolo.
MPSK esta orientado a conseguir mayores velocidades de transmisión en bits por segundo que otras modulaciones para un mismo canal.
Entre menor sea la modulación M será más inmune al ruido, ya que entre más cercanas estén las fases menos confianza se tendrá de la modulación debido al margen tan estrecho entre las fases.
Dos fases adyacentes se diferencian solo en un bit, lo que permitirá disminuir los errores en la transmisión puesto que si una fase se desplaza junto a la adyacente o a su lugar entonces solo se tendrán errores en un bit.
Las modulaciones tipo MPSK se realizan con el propósito de aumentar la eficiencia espectral mediante el uso de un numero mayor de fases. Pero por las tasas de error BER en función de la relación portadora a ruido C/R no es conveniente continuar incrementando el numero de fases PSK.

Modulación QAM
La técnica de modulación digital por amplitud de cuadratura QAM (Quadrature Amplitude Modulation) se usa para hacer los módems más rápidos, es muy utilizada por Bell y CCITT en los módems. Es una combinación de PSK y ASK por lo que combina las variaciones de amplitud en referencia al momento de fase en que ocurren con lo que se pueden incluir mas bits en los mismos hertz, permite la transmisión de tribits.
A la señal portadora se le modifica su amplitud y su fase para producir la señal QAM. Este tipo de modulación rompe la barrera que tiene PSK debido al numero de fases que pueden usarse ya que con un numero mayor a 16 fases tienden a estar muy cercana una fase de la otra.
QAM distribuye las fases no en un circulo sino en un reticulado, en bases a variaciones de amplitud y fase. Al igual que PSK es una modulación M-aria ya que para grupos de n bits se obtienen $M=2^n$ salidas diferentes.
Existen muchas variantes de la modulación QAM.

Modulación 8QAM
En la modulación Eight-QAM se usan como entrada grupos de tribits para dar una modulación $M=2^3=8$. De los tres bits, dos de ellos (Q, I) entran cada uno a un convertidor D/A junto con el tercero y su complemento (C) con los cuales se obtiene una señal PAM como se observa en la tabla 1.8.4.

I/Q	C	Señal PAM de salida
0	0	-0.541 V
0	1	-1.307 V
1	0	+0.541 V
1	1	+1.307 V

Tabla 1.8.4 Valores de la señal PAM para los bits I, Q y C

Las salidas de los convertidores entran a 2 moduladores donde se mezclan con la señal del oscilador en uno con la misma fase y en el otro con la fase a 90° desplazada.
Los valores que genera la señal PAM tanto en amplitud como en fase son mostrados en la tabla 1.8.5.

Entrada binaria (Tribits)			Señal de salida $f_{8QAM}(t)$	Señal de salida 8QAM
Q	I	C		
0	0	0	-0.541cos w_ct-0.541sen w_ct	-112.5°
0	0	1	-1.307cos w_ct-1.307sen w_ct	-157.5°
0	1	0	-0.541cos w_ct+0.541sen w_ct	-67.5°
0	1	1	-1.307cos w_ct+1.307sen w_ct	-22.5°
1	0	0	+0.541cos w_ct-0.541sen w_ct	+112.5°
1	0	1	+1.307cos w_ct-1.307sen w_ct	+157.5°
1	1	0	+0.541cos w_ct+0.541sen w_ct	+67.5°
1	1	1	+1.307cos w_ct+1.307sen w_ct	+22.5°

Tabla 1.8.5 Tabla de valores de la modulación 8QAM

Sus diagramas de fasores y constelación de puntos se observan en la Fig. 1.8.16.

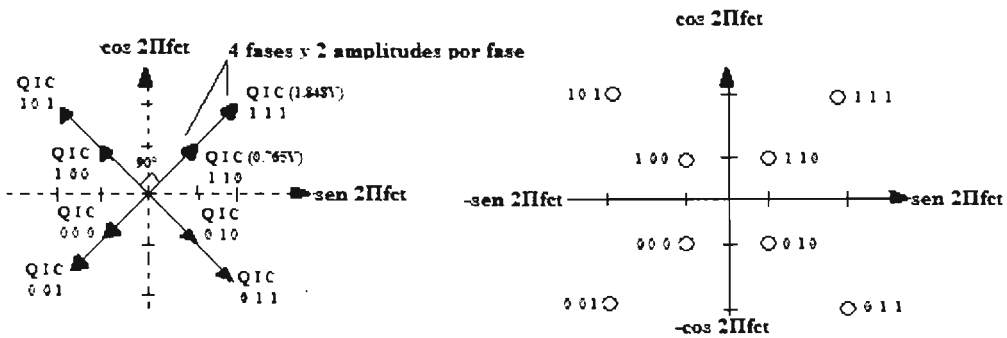


Fig. 1.8.16 Diagrama de favores y constelación de puntos de 8QAM

De la Fig. 1.8.16 se puede ver que la modulación se realiza tanto en fase como en amplitud, teniendo una separación entre fases adyacentes de 90° así como una diferencia de amplitud entre fases iguales de 1.083V.
Si se realiza una comparación de 8QAM con 8PSK vemos que tiene gran ventaja 8QAM ya que el margen de ruido permitido es mayor en esta (±45°), mientras que en 8PSK el margen es de ±22.5°, además de que se utiliza el código gray difiriendo cada fase en un solo bit.

Modulación 16QAM

La modulación Sixteen QAM (16QAM) hace una modulación M=16 por lo tanto trata los datos de entrada en grupos de n=4 bits o quadbits ($M=2^4$).

De los 4 bits cada par entra a un convertidor A/D, el cual produce una señal analógica PAM de 4 niveles de tensión, tabla 1.8.6.

I	-I	Señal PAM Canal I	Q	-Q	Señal PAM Canal Q
0	0	-0.220V	0	0	-0.220V
0	1	-0.821V	0	1	-0.821V
1	0	+0.220V	1	0	+0.220V
1	1	+0.821V	1	1	+0.821V

Tabla 1.8.6 Valores de las señales PAM generadas por los convertidores A/D

Estas señales PAM son multiplicadas en un modulador cada una, así la señal PAM del canal I se multiplica por la portadora senoidal y la señal PAM del canal Q se multiplica por la portadora defasada 90°, formando los valores de la señal 16QAM de la tabla 1.8.7

Entrada binaria (Quadbits)				Señal de salida 16QAM	Amplitud	Fase
Q	Q	I	I			
0	0	0	0	-0.220cos2Πfct-0.220sen2Πfct	0.311 V	-135
0	0	0	1	-0.220cos2Πfct-0.821sen2Πfct	0.850 V	-165
0	0	1	0	-0.220cos2Πfct+0.220sen2Πfct	0.311 V	-45
0	0	1	1	-0.220cos2Πfct+0.821sen2Πfct	0.850 V	-15
0	1	0	0	-0.821cos2Πfct-0.220sen2Πfct	0.850 V	-105
0	1	0	1	-0.821cos2Πfct-0.821sen2Πfct	1.161 V	-135
0	1	1	0	-0.821cos2Πfct+0.220sen2Πfct	0.850 V	-75
0	1	1	1	-0.821cos2Πfct+0.821sen2Πfct	1.161 V	-45
1	0	0	0	+0.220cos2Πfct-0.220sen2Πfct	0.311 V	+135
1	0	0	1	+0.220cos2Πfct-0.821sen2Πfct	0.850 V	+165
1	0	1	0	+0.220cos2Πfct+0.220sen2Πfct	0.311 V	+45
1	0	1	1	+0.220cos2Πfct+0.821sen2Πfct	0.850 V	+15
1	1	0	0	+0.821cos2Πfct-0.220sen2Πfct	0.850 V	+105
1	1	0	1	+0.821cos2Πfct-0.821sen2Πfct	1.161 V	+135
1	1	1	0	+0.821cos2Πfct+0.220sen2Πfct	0.850 V	+75
1	1	1	1	+0.821cos2Πfct+0.821sen2Πfct	1.161 V	+45

Tabla 1.8.7 Tabla de valores de amplitud y fase de la señal 16QAM

Los diagramas de fasores y constelación de puntos se muestran en la Fig. 1.8.17

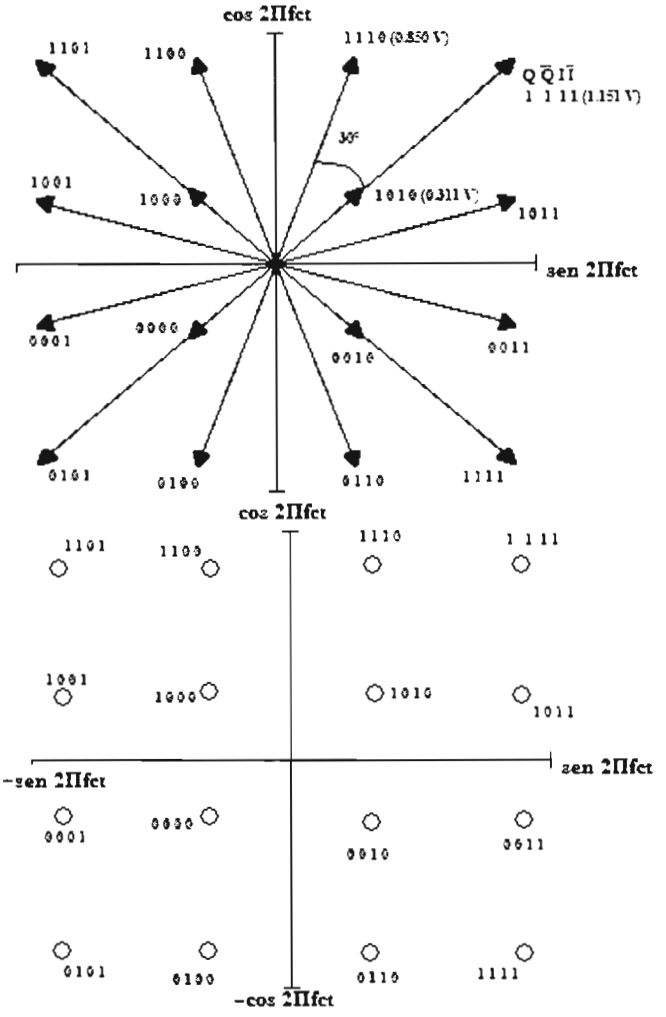


Fig. 1.8.17 Diagrama de fasores y constelación de puntos 16QAM.

Del diagrama de fasores podemos ver que la modulación 16QAM tiene una separación de 30° de fases adyacentes el cual es mayor que la modulación 16PSK.
16QAM permite transmitir a una velocidad de 140 Mbps (4x34 Mbps) en un ancho de banda de 80 MHz.

Consideraciones para la modulación MQAM.
El ancho de banda mínimo para transmitir una señal digital MQAM es:
$B_{MQAM}=2B_F$
Donde B_F es el ancho de banda de la señal digital de información f(t).
La relación entre la velocidad de transmisión en baudios (símbolos/seg) y ancho de banda de la señal digital, según la velocidad de Nyquist es:
$V_B=2B_F$
Ya que en un símbolo se transmiten k bits de información:
$V_b=kV_B$
Donde V_b es la velocidad de transmisión (en bps) de la señal digital que entra al modulador.
El ancho de banda mínimo en función de la velocidad en bps es:
$B_{MQAM}=V_b/k$

Por lo tanto en MQAM el ancho de banda mínimo para transmitir una señal MQAM es igual a la velocidad en bps a la entrada del modulador dividido por el numero de bits transmitidos por símbolo.
MQAM esta orientado a conseguir mayores velocidades de transmisión en bits por segundo que otras modulaciones para un mismo canal. Por otra parte entre menor sea la modulación M será más inmune al ruido la modulación, ya que entre más cercanas estén las fases menos confianza se tendrá de la modulación debido al margen tan estrecho entre las fases. También tenemos que se prefiere usar el código Gray para que dos fases adyacentes se diferencien solo en un bit, lo que permitirá disminuir los errores en la transmisión puesto que si una fase se desplaza junto a la adyacente o a su lugar entonces solo se tendrán errores en un bit.

Capacidad de transmisión de las técnicas de modulación digital
La capacidad de transmisión de información de un canal con un ancho de banda es igual a la máxima velocidad a la que se puede transmitir un mensaje por el canal. La velocidad de Nyquist o velocidad de transmisión en baudios por segundo V_s es igual al doble del ancho de banda de la señal digital de información.
$V_S=2B_F \Rightarrow B_F=V_S/2$
El ancho de banda de los diferentes tipos de modulación digital es:
$B_{ASK}= 2B_F= V_S=V_b$ V_b es la velocidad en bps
$B_{FSK}=2B_F+2\Delta f=V_S+2\Delta f=V_b+2\Delta f \geq V_b=V_S$
$B_{PSK}= 2B_F= V_S=V_b$
$B_{MPSK}= 2B_F= V_S=V_b/k$
$B_{QAM}= 2B_F= V_S=V_b/k$
De estos anchos de banda podemos observar que FSK es la modulación que requiere mayor ancho de banda.
Por otra parte una forma de medir la capacidad de transmisión de información de un canal es sobre la base de la eficiencia del ancho de banda ($BW_{eficiencia}$) definida como
$BW_{eficiencia}= V_B/B$
Donde B es el ancho de banda mínimo para transmitir una señal modulada.
De la formula podemos ver que la eficiencia para un canal con un ancho de banda determinado que soporta una velocidad de transmisión en baudios (V_S), cuanto mayor es la velocidad en bps (V_b) mayor será la eficiencia del canal y que por este se transmite una mayor cantidad de información en el mismo tiempo, la tabla 1.8.8 compara las velocidades en bps y la eficiencia de los diferentes tipos de modulación.

Modulación	BW mínimo de la	Núm. De bits			
	Señal modulada	En un símbolo	V_S	V_b	$BW_{eficiencia}=V_b/B$
ASK	B	1	B	B	1
FSK	B	1	$\leq$B	$\leq$B	$\leq$1
PSK	B	1	B	B	1
QPSK	B	2	B	2B	2
8PSK	B	3	B	3B	3
8QAM	B	3	B	3B	3
16PSK	B	4	B	4B	4
16QAM	B	4	B	4B	4

Tabla 1.8.8 Comparaciones de los distintos tipos de modulación en cuanto a la eficiencia.

De la tabla 1.8.8 se puede observar que las modulaciones M-arias son las más eficientes y serán mas en cuanto aumente el valor de $M=2^n$.
La comparación en cuanto a la inmunidad al ruido arroja que la modulación PSK tiene un mejor comportamiento frente al ruido y FSK es más inmune que ASK.
Por las ventajas anteriores PSK debería ser mas usado lo cual no siempre es así, debido a que ASK y FSK se pueden demodular por detección sincrona y detección de envolvente, mientras PSK solamente se pude demodular por detección sincrona, lo cual es un proceso más complejo y costoso por el hecho de tener que recuperar la portadora de la señal recibida para evitar que la portadora local no sea de la misma frecuencia o este defasada de la portadora original. Así ASK no es muy utilizado, mientras que FSK se suele usar en módems asíncronos de bajo rendimiento y bajo coste para la comunicación de datos a través de la banda de voz de la línea telefónica.

1.9 Errores en la comunicación de datos

Cuando se transmiten datos en un sistema de comunicaciones existen una serie de factores (atenuación, ruido, interferencia en el medio físico) que afectan la transmisión provocando diferencias entre las secuencias de datos enviadas a través de un canal y las secuencias de datos recibidas. Estas diferencias entre los datos transmitidos y los recibidos son los errores de comunicación. Estos errores caracterizan la calidad de la transmisión por medio de la tasa de errores la cual va mostrar una relación entre el número de bits recibidos erróneos y el numero de bits transmitidos.
Para señales analógicas el medio introduce alteraciones aleatorias que degradan la calidad de la señal. Para las señales digitales esas alteraciones producen errores de bits, esos errores pueden provocar por ejemplo que aparezca un 0 en lugar de un 1 y viceversa.
Algunas de las perturbaciones que provocan los errores son:

- La atenuación y distorsión de atenuación. Debido a que la energía de la señal transmitida es inversamente proporcional a la distancia a recorrer, entre mayor sea la distancia la energía de la señal disminuirá mas. En medios guiados la atenuación es logarítmica por lo que es expresada en dB/km. Para medios no guiados la atenuación no solo va a depender de la distancia sino también de las condiciones atmosféricas. La atenuación afecta a la comunicación de los datos por las siguientes razones: Si la señal se atenúa demasiado no podrá ser detectada por los circuitos electrónicos que necesitan un mínimo de señal; una señal atenuada hará que la calidad de la comunicación no sea aceptable y los errores se saldrán de un valor mínimo permitido; la atenuación va a crecer junto con la frecuencia a la que se transmite. Un claro ejemplo de la atenuación es cuando se realiza una transmisión en una red si el cable es demasiado largo o tiene mucha atenuación, un bit 1 que se envía desde el origen puede parecer un bit cero para el momento en que llega al destino.
- Distorsión de retardo. En los medios guiados la velocidad de propagación de la señal va a variar con la frecuencia lo que provoca que las componentes espectrales de la señal no viajen todas a la misma velocidad, por lo que las mas cercanas a la frecuencia central pueden transmitirse mas rápidamente. Debido a esto la llegada al receptor no será simultanea y algunos componentes llegaran con retraso.
- Ruido. El ruido es conformado por el conjunto de señales que se introducen durante la transmisión entre el emisor y el receptor lo que provoca apariciones de nuevas frecuencias distorsionando la verdadera señal, traslapamiento de señales adyacentes y la formación de picos irregulares que afectan a la señal transformado las ráfagas de bits lo que provoca que estos pierdan toda su información. Demasiado ruido puede corromper un bit haciendo que un 1 binario se transforme en un cero binario o un 0 en un 1 destruyendo con ello el mensaje original.
- La dispersión provoca que una señal se ensanche en el tiempo con lo cual un bit puede comenzar a interferir con el bit siguiente y se puede confundir con los bits que llegan antes o después del bit afectado.
- Fluctuación de fase de temporización. Los sistemas digitales están cronometrados o sincronizados, esto quiere decir que los pulsos de reloj controlan todo, y por ejemplo en el caso de transmisiones de red son los que hacen que la tarjeta de red transmita los bits. La fluctuación de fase se produce

cuando el host origen no esta sincronizado con el host destino, provocando que los bits lleguen un poco antes o un poco mas tarde de lo esperado, la fluctuación puede provocar errores cuando el computador que recibe los bits demorados trata de volver a unir los paquetes en un mensaje. Dicha fluctuación se puede solucionar con sincronizaciones de reloj ya sea por hardware, software o de protocolo.

- Latencia. Es la demora de una señal en su transmisión por el medio físico, lo cual se debe a que el bit aparte de que tarda una pequeña cantidad de tiempo para trasladarse, esa cantidad se ve aumentada si atraviesa dispositivos electrónicos, Lo cual se puede solucionar con el uso cuidadoso de dispositivos de red, estrategias de codificación y protocolos de capa.
- Eco. Son las repeticiones atenuadas de un mismo mensaje que regresan al equipo transmisor. Si esta señal tiene la intensidad suficiente para que la detecte el equipo de comunicaciones provoca errores.
- Perdida de línea. Es una causa grave de errores y transmisiones incompletas debido a la desconexión de la línea de unión entre el transmisor y el receptor por daños a las líneas de comunicaciones.

En la Fig. 1.9.1 tenemos una representación grafica de la generación de errores que provocan estas perturbaciones.

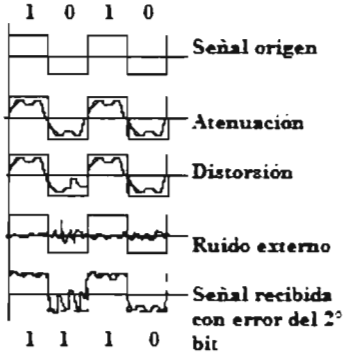


Fig.1.9.1 Perturbaciones de la transmisión.

Los errores causados por ruido se manifiestan como bits faltantes o adicionales, o como bits cuyos estados se invierten.
Algunos tipos de errores que se generan en la transmisión debido a las causas mencionar anteriormente son:

- Errores de bit. Del conjunto de datos transmitidos entre el emisor y el receptor solo cambia un bit. Este tipo de error es mas probable en la transmisión en paralelo.

- Errores de ráfaga. Se producen estos errores cuando dos o mas bits del conjunto de datos transmitido cambian, esto significa que uno o mas bits en la trama de datos son erróneos. Estos bits pueden ser consecutivos o no Esto puede darse mas probablemente en la transmisión en serie.

- Tramas perdidas. Cuando la trama que se envía no llega a su destino.

1.10 Códigos de detección y corrección de errores.

Un sistema de comunicaciones confiable debe implementar técnicas para manejar los errores, ya que es imposible tener un sistema libre de errores es necesario detectar y corregir los errores generados durante la transmisión.
Las técnicas que harán la transmisión fiable básicamente consisten en mapear (añadir redundancia) la secuencia de datos de entrada a una secuencia de entrada al canal.
Si la información a transmitir se compone de un bloque de datos de m bits, a esta se le incluye un bloque r de redundancia, con lo que la longitud final del bloque a transmitir será n, donde n=m+r.
El control de los errores de transmisión se basa en dos estrategias:

1. Usar códigos de detección de errores.
   Con la información de datos que se envía se agregan bits redundantes que ayuden a detectar la aparición de errores. Se incluye la información redundante necesaria en cada bloque de datos para detectar los errores. Una vez detectado algún error se pedirá al transmisor que retransmita la información que ha llegado con errores.
2. Usar códigos de corrección de errores.
   Con la información transmitida se agregan bits de redundancia que permiten corregir los posibles errores en la transmisión. Aquí se va a incluir suficiente información redundante en cada bloque de datos para que se pueda realizar la detección y corrección de los errores. En este caso el numero de bits de redundancia será mayor que en el caso de los métodos que solo detectan errores.

Las operaciones básicas de procesamiento de señales en un sistema de comunicación digital son codificación de la fuente, codificación de canal y modulación digital en el lado del transmisor y sus procesos inversos en el lado receptor. Los códigos para detección y corrección de errores corresponden a la codificación de canal.

Bits de redundancia
Los bits de redundancia son bits adicionales que se introducen deliberadamente a los datos que componen la información codificada que se va a transmitir, esto se realiza para que el destino pueda detectar en base a esos bits adicionales errores en la transmisión.
La redundancia de un código se define como la diferencia ente la información máxima que podría proporcionar un alfabeto empleado y la que proporciona realmente.
Un código más redundante necesitara mensajes más largos que uno con menos redundancia para transmitir la misma cantidad de información. En estos códigos redundantes los dígitos que no transportan información se usan para detectar errores e incluso corregirlos.
Para ejemplificar de manera sencilla la redundancia supongamos que queremos representar cuatro símbolos (1, 2, 3, 4) y para esto tenemos un código sin redundancia compuesto de dos bits para representarlo (00, 01, 10, 11).
Si por algún error se obtiene otro símbolo no se puede detectar. Pero si al código se agrega un bit de redundancia al final (000, 010, 100, 110), se podrán detectar algunos errores determinados. El bit de redundancia agregado a nuestro código ha sido el 0, si un error produce un cambio en el ultimo bit se detectaría que es invalido, ya que si en vez de recibir un 000 se recibe un 001, este símbolo no existe en nuestro alfabeto y de esta forma cualquiera de los símbolos que se reciba con el ultimo bit cambiado (001, 011, 101, 111) no existirá en nuestro alfabeto (000,010,100,110) y por lo tanto el símbolo recibido es erróneo.

Normalmente para llevar a cabo las tareas de detección y corrección de errores se utilizan códigos en función de los bits que componen la información a transmitir, el código indicara si se ha cambiado algún bit en la transmisión. El código utilizado debe ser conocido e interpretado tanto por el emisor como por el receptor.
El uso de los códigos para corregir errores mediante procesos algebraicos se realiza con autómatas compuestos de codificadores y decodificadores, Fig. 1.10.1

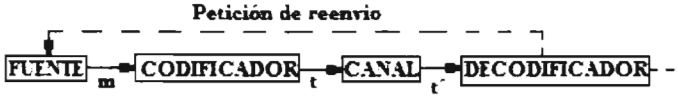


Fig. 1.10.1 Autómata de codificadores para el control de errores

En la Fig. 1.10.1 m es el mensaje a comunicar, t=m codificado con cierta información redúndate y t' será una palabra del código igual a m si no hay errores, si los hay no será una palabra del código y entonces se procede ya sea a desecharla, pedir su retransmisión o corregirla. Según la capacidad del código este podrá solo detectar ciertos tipos de errores, corregirlos o hacer ambas cosas.
Los códigos desarrollados para llevar a cabo las tareas de detección y corrección de errores se clasifican de la siguiente forma:

- Códigos sistemáticos. Son los códigos en los que la palabra de información aparece de forma explicita en la palabra codificada.
- Códigos no sistemáticos. Son los códigos en los que la palabra de información no aparece de forma explicita en la palabra codificada.
- Códigos de bloque. Códigos en los que todas las palabras tienen la misma longitud y la codificación se hace de forma estática.
- Códigos lineales. Códigos en los que cualquier combinación lineal de palabras de código valida (como la suma modulo 2) produce otra palabra valida.
- Códigos cíclicos. Códigos en los que cualquier desplazamiento cíclico de una palabra de código da lugar a otra palabra de código.

Códigos para la detección de errores
La detección de errores es un proceso que analiza la información recibida en el receptor para determinar si ha ocurrido algún error en la transmisión. Este proceso no identifica cual bit tiene errores solamente identifica que ocurrió un error. Los códigos para detección de errores pueden ser clasificados por la técnica utilizada para la detección de errores.

Tipos de códigos para la detección de errores.

Técnica del eco.
Este método es una forma muy simple de detectar errores ya que se basa en regresar del receptor al emisor la información recibida para poder compárala con la información original y determinar si hubo algún error, el cual se puede corregir reenviando los datos. Su gran desventaja es que realiza dos veces la misma transmisión.

Códigos de detección automática mediante suma de comprobación o checksum.

Los códigos de comprobación de suma son de los códigos más simples que usan la técnica de detección automática agregando a los datos un marco de verificación de secuencia o FCS (Frame Check Sequence), el FCS se obtiene a partir de los datos a transmitir mediante un algoritmo. Cuando se recibe el mensaje el receptor aplica el mismo algoritmo a los datos recibidos y compara el FCS que el obtuvo con el agregado a los datos, si son iguales, el mensaje llego correctamente de lo contrario hubo algún error.

Código de verificación de paridad vertical

Los códigos de comprobación de redundancia vertical VRC (Vertical Redundacy Check) permiten verificar la paridad de los bits de un carácter por lo que también se conoce como paridad de carácter. La técnica de paridad consiste en agregar un bit extra (bits de paridad) a un carácter o un bloque de caracteres formado por n bits para forzar al total de unos (1) en el código a ser par (código de paridad par) o impar (código de paridad impar) y de esta manera poder detectar los errores en la validación de los datos. El bit de paridad puede ser cero o uno. Esta técnica de paridad se puede aplicar en dos formas:

- Código de paridad par. Si hay un total de 1´s impar se agrega un bit 1 para que el total de bits 1 sea par, si el total de 1´s es par se agrega un 0 para no alterar la paridad par. Por ejemplo si se quiere transmitir el flujo de bits 1100001. Agregamos un bit 1 para tener una paridad par, así lo que se transmite será 11000011. Si al receptor llega por ejemplo un flujo 11000111, este detectara que hay un error de paridad, ya que el numero de 1´s no es par. Este tipo de paridad normalmente se aplica para la transmisión sincrona.
- Código de paridad impar. Si hay un numero total 1´s par se agrega un bit 1 para hacer que el numero total de bits 1 sea impar, si el total de 1´s ya es impar se agrega un 0 para no alterar la paridad impar. Para ejemplificar esto si para transmitir un flujo de 1100011 se agrega un bit 1 para hacer la paridad impar, entonces se transmite 11000111, si el receptor llegase a recibir un 11100111 detectara que la paridad no es impar como se acordó con el transmisor. Este tipo de paridad normalmente se aplica para la transmisión asíncrona.

Normalmente el bit de paridad se agrega a la izquierda del carácter original.

Este método permite detectar el error pero no nos dice donde se encuentra el error, además de que no detecta los errores de mas de un bit, es decir nos indica que la paridad acordada cambio pero no se sabe si este cambio se debió a 2, 3 o más errores, solo sabemos que la paridad de 1´s es par o impar, estas técnicas solo detectan un único error, y cumple satisfactoriamente su objetivo si los errores no cambian un par de bits a la vez. Puede suceder que el mismo bit de paridad sea alterado por el ruido o incluso que más de un bit de datos sea alterado con lo cual este sistema de detección falla. Por ejemplo si se transmite un carácter con paridad par 10100000 y se recibe 01010000, vemos que los 4 primeros bits están alterados pero sin embargo la paridad sigue siendo par, como se cumple la paridad el sistema creerá que no hay ningún error, es aquí donde este método falla.

Código de verificación de redundancia longitudinal

Los códigos de comprobación de redundancia longitudinal LRC (Longitudinal Redundancy Check) determinan si ha ocurrido un error durante la transmisión de un mensaje por lo que se conoce como paridad de mensaje, estos códigos arreglan un bloque de bits a transmitir en filas y agregan una fila de redundancia para hacer que los bits 1 en cada columna tengan una paridad par o impar, como muestra la Fig.1.10.2

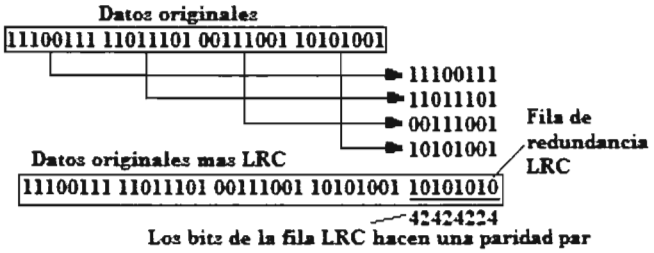


Fig. 1.10.2 Detección de errores por LRC

El método LRC puede detectar y corregir un error en un bit, puede detectar errores en dos bits pero no los corrige. Puede que no detecte algunos errores como por ejemplo que algún 1 sea detectado por 0 en una columna y un 1 por 0 en la misma con lo cual el receptor vera la paridad como se acordó y creerá que no hay errores cuando en realidad dos bits fueron alterados.

Código de redundancia cíclica

Los códigos de comprobación de redundancia cíclica CRC (Check Redundancy Cyclic) o códigos polinómicos son buenos para la detección de errores. Como se ha visto los métodos VRC y LRC se basan en sumar el numero de 1´s existentes en un bloque de datos para incluir redundancia, a diferencia de ellos el CRC utiliza la división binaria. Tratan con polinomios con coeficientes de valor 0 o 1 y que representan cadenas de bits. Por lo tanto las tramas de n bits se representan como los coeficientes de un polinomio de grado n-1, asimismo hace uso de un polinomio generador G(x) (acordado previamente entre el emisor y el receptor) de grado r. Tanto los bits mayor cómo menor del polinomio deben ser 1. El grado del polinomio generador debe ser menor que el polinomio que representa a la información. A partir de estos componentes se debe obtener una suma de comprobación la cual se va a sumar al polinomio de información y juntos se transmitirán al receptor. Esa suma de comprobación ayuda a determinar si hay algún bit erróneo en el mensaje transmitido. El polinomio del mensaje mas la suma de comprobación debe ser divisible entre el polinomio generador y si el residuo es diferente de 0, ha habido un error de transmisión.

La elección del polinomio generador es esencial si se quiere detectar la mayoría de los errores. Normalmente se usan polinomios G(x) generadores del CRC estandarizados, los cuales son escogidos por sus propiedades que ayudan a detectar errores, por ejemplo algunos polinomios estándares son:

CRC-12 = $x^{12}+x^{11}+x^3+x^2+x^1+1$

CRC-16 = $x^{16}+x^{15}+x^2+1$

CRC-CCITT = $x^{16}+x^{12}+x^5+1$

CRC-32 = $x^{32}+x^{26}+x^{23}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Con la elección de un polinomio generador adecuado los siguientes errores tienen patrones que no son divisibles por el y por lo tanto son detectables:

- Todos los errores de un bit.
- Todos los errores dobles, si G(x) tiene al menos tres 1´s.

- Cualquier número impar de errores, siempre que G(x) contenga e factor x+1
- Cualquier error a ráfagas en el que la longitud de la ráfaga sea menor que la longitud del polinomio divisor, o sea la longitud de la secuencia de comprobación de trama FCS. Un error de ráfaga empieza con un 1 inicial, una mezcla de ceros y unos, y un 1 final.
- La mayoría de las ráfagas de mayor longitud.

El polinomio CRC-16 permite detectar errores simples, dobles, en números impares de bits, en ráfagas de 16 y 18 bits. En la detección CRC también se presenta el problema de que algunos errores no pueden ser detectados.
Los códigos de redundancia cíclica son buenos para la detección de errores. Se diseñan para detectar muchas combinaciones de errores, ya que detectan los errores de ráfaga de un numero impar de bits, los errores de ráfaga de longitud menor o igual que n y detecta con probabilidad muy alta, los errores de ráfaga con longitud mayor que n, son muy usados en la practica debido a su sencillez de implementación.

Códigos de corrección de errores
El uso de códigos de corrección de errores trata de detectar y corregir los errores aparecidos en las transmisiones, ya que el añadir un único bit de paridad no garantiza la integridad de los datos ni es suficiente para datos que se transmiten a distancias muy largas (como la transmisión de datos entre PC´s por Internet, donde la comunicación puede ser de un lado del mundo al otro) puesto que están demasiado expuestos a interferencias eléctricas. De estos problemas se derivo el desarrollo de códigos que detectan mas de un error e incluso corrigen los errores que encuentran. Los códigos de corrección de errores pueden ser clasificados según el método usado para corregir errores.

Métodos para corregir errores.

Retransmisión.
Detección de errores o corrección hacia atrás ARQ. El método de solicitud de repetición automática solicitud de confirmación ARQ (Automatic Repeat Query o Acknowledgment Request) o corrección hacia atrás es usado para el control de errores en la transmisión de datos, garantizando la integridad de los datos, consiste en la retransmisión de la información afectada por los errores, es un método simple y solo retransmite si hay errores detectados por el receptor el cual solicita la repetición de los bloques de datos al emisor y este ultimo los retransmitirá tantas veces como sea necesario hasta que se reciban sin errores, en caso de que la transmisión haya sido exitosa sin errores simplemente se regresa una confirmación de recepción correcta. Este sistema usa un canal de retorno (canal hacia atrás), cuando se detecta un error el receptor lo indica al transmisor sobre el canal hacia atrás y se transmite de nuevo el bloque de información que contiene el error. Es uno de los métodos más confiables para la corrección de errores, aunque no es el más eficiente. El método ARQ utiliza las siguientes técnicas para controlar la información:

- Confirmaciones positivas. Si el receptor recibe la información correctamente devuelve una confirmación ACK (acknowledge) de cada trama recibida correctamente.
- Retransmisión después de la expiración de un intervalo de tiempo. Ya que los mismos reconocimientos se pueden perder se maneja un tiempo prefijado (timeout) durante el cual el receptor espera y si ese tiempo expira sin recibir una confirmación por parte del receptor retransmite la información automáticamente.

- Confirmación negativa y retransmisión. El receptor responde con NACK si no recibió correctamente la información y el emisor la vuelve a reenviar.

ARQ suele usarse en sistemas que no actúan en tiempo real (voz y video) ya que el tiempo que se pierde en el reenvió puede ser considerable, en estos casos es mejor emitir mal en el momento que correctamente un tiempo después, pues en una videoconferencia no es muy útil emitir el píxel correcto de la imagen 2 segundos después de haber visto la imagen.

Seguimiento de corrección de errores.

El método de seguimiento de corrección de errores FEC (Forward Error Correction) o corrección hacia delante se basa en enviar los suficientes bits de paridad para reconocer la información afectada por errores y de esta manera los códigos autocorrectores permiten corregir los errores de transmisión en el receptor sin pedir retransmisión.. El propósito de los códigos FEC es reducir o eliminar el tiempo gastado en retransmisiones. Se usa en sistemas sin retorno o de tiempo real en los que no se puede esperar a una retransmisión para mostrar los datos ya que por ejemplo en transmisiones a muchos receptores los reconocimientos no son prácticos. Funciona evaluando el síndrome del vector recibido al cual se asocian varios errores y se toma el más probable Para recuperar el mensaje original se suma el error calculado al vector recibido con lo cual se puede cancelar el efecto. Hay un gran numero de códigos tipo FEC para corregir errores, los cuales serán usados sobre la base de la relación entre la redundancia, la reducción de la tasa de errores de bit (BER) y la complejidad del hardware, sus variantes son:

- FEC de bloques. Las variantes de bloques mas usadas son BCH y RS (Reed-Solomon).
- FEC convolucional. En este método se aplica el algoritmo de Viterbi.

En la corrección de errores con acción hacia delante FEC se usan códigos binarios diseñados para corregir por si mismos los errores introducidos en la transmisión, con lo que en la estación receptora se pueden reconstruir los mensajes que contengan error.

Códigos de Bloques

En los códigos de bloque se toman k bits de información cada vez y se añaden c bits de paridad, la verificación se hace sobre las combinaciones de los k bits de información, un bloque consta de n=k+c dígitos, el código consta de k palabras cada una con n dígitos de extensión.

La efectividad de los códigos de bloque depende de la diferencia entre una palabra de código valida y otra, cuanto mayor es esta diferencia menor es la posibilidad de que un código valido se transforme en otro debido a los errores. Esta diferencia es conocida como la distancia de Hamming.

Distancia de Hamming

La distancia de hamming entre dos códigos es el número de símbolos o bits en que se diferencian.

O en términos de los 1´s que componen una palabra. El peso de una palabra es el numero de 1´s que contiene, Entonces la distancia de Hamming será el peso resultante de la suma en modulo 2 (sin acarreo) de las dos palabras de código.

Dos palabras serán más fáciles de distinguir entre mayor sea su distancia de Hamming. Esta distancia de Hamming nos indica el numero de bits que tienen que cambiarse para

transformar una palabra de código valida en otra palabra de código valida. Así si dos palabras difieren en una distancia d, se necesitan d errores para convertir una en la otra. El análisis de la distancia de Hamming revela que la eficacia de un código será función de la distancia de Hamming.
Estos códigos cumplen las siguientes propiedades:

- Un código de distancia mínima de Hammning d detectara d-1 errores
- Un código de distancia mínima d corregirá (d-1)/2 errores.
- La suma modulo-2 de dos palabras del código da lugar a otra palabra del código.

La notación para especificar estos códigos es:
(n, k)
Donde:

- n es el tamaño de la palabra codificada.
- k es el tamaño del mensaje original. Estos bits se transmiten sin alterarse.
- n-k son los bits de redundancia, mediante os cuales se detectan y corrigen errores.

Los códigos de boque estructuran los datos en bloques de longitud fija y le añaden a cada bloque bits de redundancia. Esos bits que se añaden solo deberán formar ciertas combinaciones de bits para formar palabras de código validas. Así si la transmisión es correcta no hay mas problema. Pero si no, el código no es valido y habrá dos posibilidades:

- Que se aplique un código autocorrector para que el receptor reconstruya el bloque original.
- Qué se aplique un código de autochequeo para que el receptor pida que se retransmita el bloque.

Códigos de Bloque usando paridad horizontal y vertical

Algunos códigos de bloque combinan el chequeo de la paridad horizontal y vertical (LRC y VRC) para detectar errores en la transmisión de los datos, Fig. 1.10.3. Para realizar esto se agrupan los caracteres en bloque. Entonces se calcula el bit de paridad para cada fila y para cada columna, por lo tanto el bloque resultante tendrá una columna y una fila mas que el bloque original. Donde la nueva columna se formara con los bits de chequeo de paridad horizontal y la nueva fila con los bits de chequeo de paridad vertical. Y además se agrega un bit de paridad cruzada, calculado a partir de la paridad de los bits LRC y VRC (Paridad LRC+Paridad VRC). Si se quiere transmitir la palabra PAG en ASCII, los caracteres en hexadecimal serán P=50=1010000; A=41=1000001; G=47=1000111, se agrupan en un bloque fig. 1.10.3

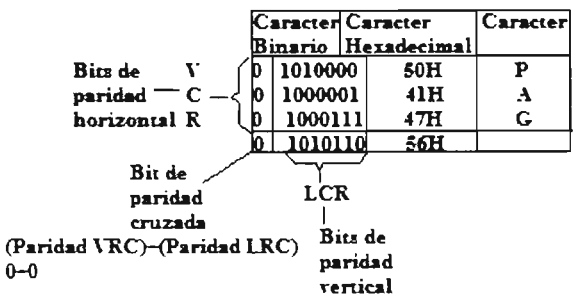


Fig.1.10.3 Formación de un código de bloques

De la Fig. 1.10.3 podemos ver que entonces se transmitirá un bloque formado por cuatro filas y nueve columnas con los caracteres 50, 41, 47 y 56 (01010110).

En este código la distancia de Hamming es de 4; con lo que si cambia un bit, cambiaria un bit del VRC, uno del LRC y 1 del bit de paridad cruzadas, o sea 4 bits en total.
Este error detectara d-1=4-1=3, errores simples, dobles y triples. Corrige (d-1)/2=(4-1)/2=1 error simple.
La transmisión del bloque total se realiza secuencialmente por filas y en el receptor se reconstruye la matriz para la detección de los errores.

Código BCH (Bose-Chaudhuri Hocquenghen).
Es un código cíclico conveniente para errores independientes. Este es un código con una gran variedad de parámetros tales como:
- Longitud de bloque $N=2^M-1$ para $M\geq 3$
- Bits de información I=N-M.t
- Distancia mínima d=2.t+1

Para $m\geq 3$ y $t<(2m-1)$ se tienen algunos códigos BCH con los siguientes parámetros:
Para tamaños de unos cientos de bits o menos, estos códigos son de los mejores para un mismo tamaño de bloque e índice de código. Algunos códigos comunes en la forma (n, k, t), son: (7, 4, 1), (15, 11, 1), (15, 7, 2).
Este código es usado en la tecnología celular analógica AMPS. En codificadores digitales de TV a 34 Mbps para corregir 2 errores por bloque, así como en el servicio TDMA

Código Reed-Solomon RS
El código Reed-Solomon es una subclase de los códigos BCH no binarios y es muy apropiado para ráfagas de errores. Se distingue de los códigos binarios por que este opera con símbolos de b bits cada uno, en lugar de bits individuales. Es útil cuando los errores ocurren en ráfagas, como en los sistemas de grabación de los CD's. Los parámetros que define son:
- Bits por símbolo: m
- Longitud del bloque: $N=m.2^m-1$ simbolos
- Símbolos de paridad: $(N-I)=m.2^t$ simbolos
- Tamaño del mensaje: k símbolos
- Distancia mínima: d=m.(2.t+1) símbolos
- Errores a corregir: t símbolos

El numero de errores en general corregidos por este código son t ráfagas de m bits en una palabra de código.
Se puede aplicar en radio enlaces digitales de 140 Mbps para corregir 4 errores en 4 bloques.

Código de convolución.
El código de convolución usado para detección y corrección de errores se enrolla o se convoluciona sobre otro, es la convolución de una corriente de datos y la función de respuesta de un codificador.

Código Hagelberger
El código Hagelberger es un código de corrección de errores con acción adelante que combate con eficacia las ráfagas de error. Para cumplir con su función requiere que se cumplan dos requisitos: que la longitud de la ráfaga no sea de mas de 8 bits y deben existir por lo menos 91 dígitos correctos entre ráfagas.

1.11 Protocolos de comunicaciones.

Los protocolos de comunicaciones permiten la comunicación entre dos entidades situadas en sistemas diferentes las cuales necesitan interconectarse para intercambiar algún tipo de información. Un protocolo se va a definir por los siguientes puntos:
- La sintaxis: La cual define el formato de los datos y los niveles de las señales.
- La semántica: incluye información de control para la coordinación y manejo de errores.
- La temporización: incluye la sincronización de velocidades y secuenciación.
- Estas tareas se subdividen en subtareas y forman una arquitectura del protocolo.

Concepto de protocolo
Un protocolo es un conjunto de normas y reglas que controlan la transmisión y recepción en la comunicación de datos entres dos o más entidades, mediante el uso de formato y la sincronización relativa del intercambio de mensajes.
Los protocolos permiten iniciar, mantener y terminar un dialogo entre elementos del sistema, controlaran el momento en que deben generarse o interpretarse los elementos orientados al control de errores y la forma de recuperar los datos recibidos con errores. También proporciona información para identificar el camino usado para el intercambio de información e identificación del tipo de mensaje.
En la comunicación entre computadoras o redes de computadoras el protocolo debe definir las reglas, convenios, funciones utilizadas, etc. para la comunicación por medio de la red.
Los protocolos de comunicaciones normalmente forman una arquitectura de niveles para reducir la complejidad de la comunicación de datos agrupando lógicamente ciertas funciones en áreas de responsabilidad o niveles. Las características de cada nivel son las siguientes:

- Cada nivel provee servicios al nivel superior y recibe servicios del nivel inferior.
- Un mensaje proveniente de un nivel superior contiene una cabecera con información a ser usada en el nodo receptor.
- El conjunto de servicios que provee un nivel es conocido como una entidad y cada entidad consiste en un manejador y un elemento.

Los protocolos pueden ser clasificados según el nivel donde son aplicados, así tendremos:

- Protocolos en el nivel de enlace
- Protocolos en el nivel de red
- Protocolos en el nivel de transporte
- Protocolos de aplicación

Cada nivel del protocolo le transmite los datos al siguiente nivel y este le agrega datos propios de control para posteriormente volver a transmitir el conjunto al siguiente nivel. Cada nivel forma unidades de datos que contienen los datos tomados del nivel anterior junto a datos propios de este nivel y al conjunto obtenido se le llama PDU (unidad de datos de protocolo).

Protocolos de nivel de enlace
Los protocolos de nivel de enlace de datos controlan la comunicación correspondiente al nivel de enlace de datos, (el nivel de enlace de datos es el conjunto de 2 equipos terminales de datos mas los elementos que componen la red de transmisión que permiten el intercambio de información, el enlace de datos puede ser punto a punto, multipunto o serial), el protocolo de enlace de datos proporciona un conjunto de

procedimientos para el establecimiento, mantenimiento y la desconexión de los circuitos para el envío de bloques de información, controla que la transferencia de datos sea correcta y coordina los métodos para la detección y corrección de errores.
El protocolo del nivel de enlace debe cuidar mediante sus procedimientos que la transmisión y recepción de tramas entre usuarios directamente conectados se realice de forma confiable.
Algunas funciones de los protocolos de enlace de datos son:
- Iniciación. El protocolo envía tramas de control entre las estaciones enlazadas para checar que ambas estén disponibles para transmitir o recibir información.
- Identificación. Se envían tramas de identificación entre las estaciones para que se reconozcan mutuamente.
- Terminación. Una vez que los datos han sido transmitidos y recibidos correctamente se realiza la desconexión del enlace para liberar los recursos en ambos extremos.
- Sincronización. Se implementa algún proceso para sincronizar el envío y recepción de los octetos de información.
- Segmentación y bloqueo. Se dividen los mensajes largos en varias tramas y los cortos se unen en una trama para adaptarlos a algún formato y para que se optimice el uso del enlace.
- Sincronización de trama. Se define y diferencia una trama del resto de la información agregándole información de control que indica donde empieza y termina, para ello se pueden usar caracteres especiales para indicar el principio y fin de trama como un guión o se puede agregar un carácter de principio de trama mas un contador que indica el numero de caracteres de la misma.
- Transparencia. Esta función elimina la posibilidad de que se malinterpreten los bits de información similares a los de algún elemento de control.
- Control de errores. Se detectan y corrigen los errores mediante el uso de códigos de detección y corrección de errores como FEQ, ARQ, etc.
- Control de flujo. Con esta función se controla el envío de tramas para asegurar que el receptor tiene recursos suficientes para recibir la información transmitida, para ello se pueden implementar diferentes técnicas como:
    - Parada y espera. Se envía una trama y se espera una señal de reconocimiento ACK (Acnowledgement) para poder enviar la siguiente trama.
    - Parada y arranque. Se envían tramas hasta que el receptor envía una señal de paro, y se vuelve a empezar la transmisión cuando el receptor envíe otra señal.
    - Ventana deslizante. El receptor autoriza en cada instante el envío de un determinado numero de tramas, renovando dicho permiso según este disponible para recibirlas.
- Recuperación de anomalías. Se controlan situaciones imprevistas durante la transmisión y hacen un limitado numero de reintentos para normalizar la situación durante ciertos periodos de tiempo.
- Coordinación de la comunicación. Establece procesos para que no existan conflictos en el establecimiento de los enlaces entre estaciones que lo soliciten mediante métodos como:
    - Coordinación centralizada. Una estación principal controla el intercambio de información sondeando cada cierto tiempo a las estaciones para recibir su información, una estación secundaria no puede transmitir hasta que la principal no se lo autorice.
    - Contienda. Cualquier estación solicita información en cualquier momento mediante el uso de procedimientos para solucionar situaciones de colisiones debido a la compartición del medio.

Los protocolos del nivel de enlace básicamente se clasifican en los dos siguientes:

- Protocolos orientados a carácter.
- Protocolos orientados a bit.

Protocolos orientados a carácter.

Un protocolo orientado a carácter usa un código para la transmisión de la información con lo cual ciertos caracteres establecen el control de la comunicación. Las tramas de información se hacen acompañar de tramas de control.

Por lo tanto los mensajes se componen de un conjunto de caracteres de un determinado código, cada carácter, tanto de información como de control tiene un significado único. Los códigos mas usados por este tipo de protocolos para llevar a cabo el control son el ASCII y el EBCDIC. Los caracteres de control se clasifican en tres categorías según su función:

Delimitadores de bloque:

- SYN (Syncronous Idle). Mantienen el sincronismo en la transmisión de los caracteres.
- SOH (Start of Heading). Indica el principio de un mensaje integrado por caracteres.
- STX (start of text). Indica el comienzo de un bloque de información dentro de un mensaje.
- ETX (End of text). Indica el final de un bloque y el final del mensaje.
- ETB(end of transmission block). Indica el final de un bloque al que le siguen otros bloques.

Controladores de dialogo entre estaciones:

- EOT(end of trasmisión) Indica que la transmisión ha terminado y se puede liberar el enlace
- ENQ (Enquiry). Indica que se desea respuesta de la estación con la que se quiere establecer el enlace.
- ACK (Affirmative Acknowledge). Indica que se ha recibido bien un bloque de información.
- NAK (negative Acknowledge). Indica que se ha recibido mal un bloque de información.

Transmisión transparente

- DEL (Data link Scape). Cambia el significado de los caracteres de control que le siguen para que las estaciones puedan enviarse información coincidente con los propios caracteres de control.

Un ejemplo de un dialogo entre dos estaciones se muestra en la Fig.1.11.1

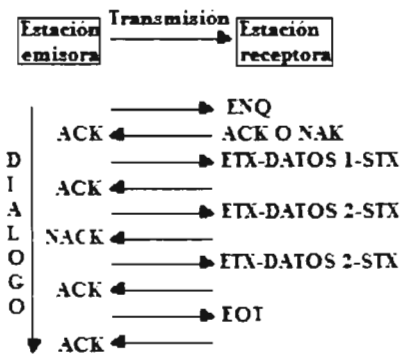


Fig. 1.11.1 Uso de los caracteres de control en un dialogo en la capa de enlace.

El dialogo entre las dos estaciones comienza con el establecimiento del enlace. En un enlace punto a punto el emisor envía al receptor un ENQ, si la receptora esta lista para recibir devuelve un ACK o sino un NAK. Si el emisor recibe un NAK espera cierto tiempo para volver a intentarlo. En un enlace multipunto la estación principal hace un sondeo, si la secundaria desea contestar manda un STX o SOH o de lo contrario un EOT. El enlace se establece por selección en caso contrario la primaria selecciona una secundaria para pasarle la información, si esta acepta devuelve un ACK o sino un NAK. El final de cada transmisión se indica con la señal ETX o ETB. El enlace se libera con una señal EOT del emisor al receptor.

Ejemplos de estos este tipo de protocolos son el BSC (Binary Synchronous Communications) de IBM, el SLC para empresas de transporte aéreo, PPP para la conexión a Internet.

Protocolos orientados a bit.

Son protocolos más modernos que los orientados a carácter los cuales surgen debido a las dificultades que tenían en ciertos casos los orientados a carácter. En estos protocolos los bits por si solos proporcionan información, lo que permite a este tipo de protocolos ser muy eficientes y trabajar con tramas de longitud variable

Algunas ventajas de estos son: son independientes del código utilizado, eficientes en la transmisión ya que la relación entre los bits de información y los de control es muy alta, alta confiabilidad en la transmisión de información puesto que se dispone de métodos de control para la detección y recuperación de errores con eficacia.

Algunos protocolos de este tipo son:

- HDLC (high-level Data link control) de ISO.
- ADDCP (Advanced Data Communications Control Procedures) de ANSI.
- LAPB (Link access procedure Balanced) del CCITT.
- SDLC (Synchronous Data Link Control) de IBM.
- BDLC (Burroughs Data Link Control) de Burroughs.
- UDLC (Data Link Control Univac) de Univac.
- LAP-B o X25 nivel 2 y LLC (Logical Link Control).
- ISO 7776.
- La capa de enlace X25 de ITU.
- Como protocolos de la subcapa MAC están los IEEE 802.3 para ethernet, IEEE 802.4, IEEE 802.5 Token Ring o el ISO 9314 para FDDI.
- El protocolo de subcapa LLC de todas las redes locales tipo broadcast es el IEEE 802.2.

Ejemplos de protocolos enlace muy utilizados son:

Protocolo SLIP

Es un protocolo muy sencillo del tipo extremo a extremo ya que ambos extremos son iguales de activos en la comunicación. En este protocolo una estación transmite paquetes IP delimitándolos con el carácter especial 0xO al final de la trama, si este byte aparece entre los datos se usa la técnica de relleno enviándose dos bytes (0xDB y 0xDC) en su lugar. Si estos vuelven a aparecer en los datos se vuelve a efectuar un nuevo relleno.

fue muy utilizado pero cayo en desuso por inconvenientes como:

- Se deja la responsabilidad de implementar mecanismos de detección y corrección de errores en los niveles superiores, ya que debido a su sencillez no proporciona dichos mecanismos.
- Solamente reconoce IP.
- Cada extremo que se desea comunicar mediante SLIP debe conocer cual es la dirección IP del otro, por lo tanto se requieren IPs fijas lo cual es un problema actual debido a la escasez de direcciones.
- No tiene ningún mecanismo que verifique la autenticidad del usuario.
- No es un estándar por lo que existen diferentes versiones no compatibles que no se pueden interconectar.

Protocolo PPP

El protocolo punto a punto PPP (Point to Point Protocol) es un protocolo orientado a carácter por lo que las tramas tienen un número entero de bytes.que maneja tasas de datos desde las mas bajas a las mas altas y es compatible prácticamente con cualquier tecnología de redes.

Este protocolo toma prestado parte del control de enlace de datos de HDLC para su interfaz con el nivel inferior por lo cual puede usarse en líneas seriales asíncronas. Este protocolo se convirtió en el más usado después de SLIP por las siguientes características:

- Es compatible con controladores estándar de HDLC.
- Puede ser usado solo en enlaces punto a punto.
- Convive con otros protocolos del tipo HDLC sobre el mismo enlace si usan direcciones.
- Puede usarse en líneas que tengan control de flujo por software.
- Tiene mecanismos de detección de errores más potentes que HDLC. Posee un método para delinear el final de un marco y el inicio del siguiente, el formato del marco también maneja la detección de errores.
- Puede negociar direcciones IP en el momento de la conexión.
- Posee mecanismos de verificación de la autenticidad.
- Delimita sin ambigüedades el final de un marco y el inicio del siguiente.
- Tiene un protocolo de control de enlace LCP (Link Control Protocol) para activar líneas, probarlas, negociar opciones y desactivarlas cuando ya no se usan.
- Posee un protocolo de negociación de red NCP (Network Control Protocol) para cada capa de red reconocida con el cual negocia opciones de la capa de red independientemente del protocolo de red usado.
- Para los protocolos de nivel de red tiene una interfaz orientada a paquetes y puede proporcionar secuenciamiento y confiabilidad.
- Posee tres tipos de entramado estándar para su uso en distintos medios: HDLC asíncrono, HDLC bit sincrono y HDLC octeto sincrono.

El formato de la trama PPP es el mostrado en la Fig. 1.11.2

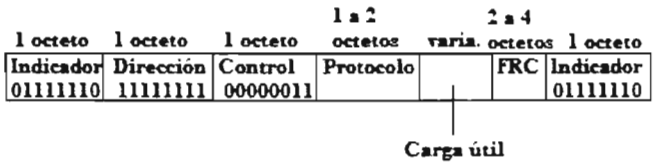


Fig.1.11.2 Formato del entramado PPP

El marco de control es un valor predeterminado por que PPP no tiene transmisión confiable (no hay números de secuencia y acuses de recibo).

El campo de protocolo indica la clase de paquete que va en la carga útil, por lo que se tienen códigos para LCP, NCP, IP, IPX, Appletalk y otros. La longitud del campo de carga se puede negociar.
Las fases de establecimiento de conexión con PPP se muestran en la Fig. 1.11.3:

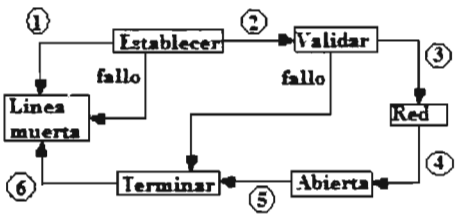


Fig. 1.11.3 Fases de establecimiento de conexión de enlace PPP

1. Cuando se detecta la portadora es por que se ha realizado una conexión en el ámbito de capa física y la conexión esta en la fase establecer. Hasta entonces la línea esta en reposo o muerta ya que no había conexión.
2. Se negocias las opciones LCP, y si hay acuerdo se procede a validar.
3. Al entrar en la fase de red se invoca al protocolo NCP apropiado para configurar la capada red.
4. Después se pasa a la fase abierta y comienza el transporte de datos.
5. y 6. La conexión pasa a al fase de terminar y vuelve a entrar en reposo la línea.

El protocolo PPP es muy utilizado en Internet para la transferencia de datos entre computadoras y para la transferencia de datos entre routers, satélites, etc.

Protocolo HDLC
El protocolo de control de enlace de alto nivel HDLC (High-Level Data Link Control) es un protocolo estándar orientado a bit de la ISO que proporciona una amplia variedad de funciones y aplicaciones, usa el control de flujo por ventana deslizante. esta considerado como un protocolo que engloba a muchos otros protocolos como SDLC, LAP, LAPB, LAPD, LAPX y LLC.
Es un protocolo transparente al código, por lo que no usa ningún código en particular para el control de línea, ya que para ello usa una secuencia de señalización al principio y fin de trama.
Las estaciones pueden estar en estado de desconexión lógica (LDS) por lo cual no puede transmitir ni recibir información, estado de inicialización (IS) o estado de transferencia de información (ITS) permitiendo a cualquier estación transmitir o recibir información, mientras este en este estado se puede emular cualquiera de los siguientes modos:

- Modo de respuesta normal (NRM). La estación secundaria debe esperar la autorización de la primaria para poder transmitir, cuando le es permitido transmite toda su información hasta la ultima trama, cuando ha terminado debe esperar nuevamente a que se le otorgue permiso.
- Modo de respuesta asíncrona (ARM). La estación secundaria transmite sin autorización si el canal esta desocupado.
- Modo asíncrono balanceado (ABM). Las estaciones combinadas comienzan las transmisiones sin permiso de las otras.

Los formatos de las tramas HDLC pueden ser de tres tipos, Fig. 1.11.4 dependiendo de su campo de control:

- Tramas con formato de información. Transmiten datos de usuario, aceptación de los datos pueden funcionar por ejemplo como comando de sondeo (poll).
- Tramas con formato de supervisión. Entre otras funciones aceptan o confirman tramas o solicitan una interrupción temporal de la transmisión de las mismas.
- Tramas con formato numerado. Realizan funciones de control como inicializar un enlace, para desconectarlo. Incluyen 5 posiciones de bits que permiten definir hasta 32 comandos y 32 respuestas.

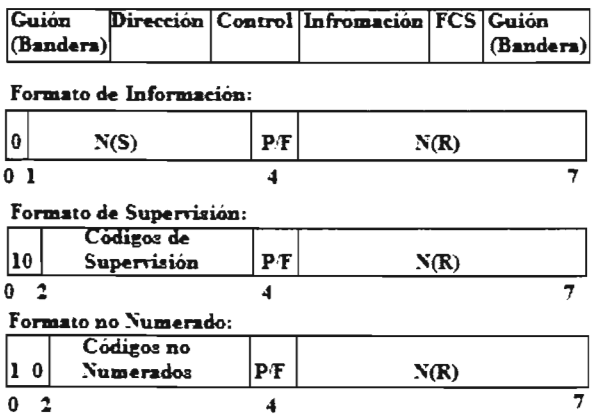


Fig. 1.11.4 Formato de la trama HDLC y sus tipos de campo de control

La trama HDLC contiene 5 o 6 campos

- Campo de señalización (banderas, guiones,....). La secuencia de señalización es 01111110. Siete unos seguidos indican un problema en el enlace. Quince unos seguidos hacen que el canal permanezca inactivo. Cuando la estación detecta una secuencia diferente a la de señalización sabe que es el comienzo de una trama, una condición de error o de canal desocupado. Cuando se encuentre la siguiente trama de señalización sabe que la trama ha llegado completa.
- El campo dirección indica la dirección que tiene asignada cada estación.
- El campo de control contiene tanto los comandos y respuestas como los números de secuencia que se utilizan para llevar a cabo la contabilidad del flujo de datos que atraviesa el enlace entre las estaciones.
- El campo de información. Contiene a los datos de usuario
- El campo de comprobación de secuencia de la trama indica si ha aparecido algún error durante la transmisión. El emisor calcula los datos de usuario y añade a la trama el resultado del cómputo, colocándolo en el campo FCS. El receptor realiza el mismo cálculo y si coinciden es probable que no hay error. El calculo para encontrar el valor de FCS es mediante la comprobación de redundancia cíclica CRC

Este protocolo es muy versátil ya que se puede implementar en transmisiones duplex y semiduplex, en enlaces punto a punto o multipunto, en canales conmutados o no conmutados.

Protocolos de nivel de red

Los protocolos de nivel de red manejan la información de direccionamiento y encaminamiento, comprueban los errores y las peticiones de retransmisión, proporcionan los procedimientos para el acceso a la red cuando la red usada los especifica como Ethernet, algunos ejemplos de protocolos de red son:

- El protocolo de conexión de red avanzada APPN (Advanced Peer-to-peer Networking) de IBM.
- Protocolo de servicio de red orientado a la conexión CONS (Connection Oriented Netwok Service) y servicio de red no orientado a conexión CLNS (Conectionless Network Service).
- Protocolo de Internet del grupo de protocolos TCP/IP de Internet y Unix.
- El protocolo IPX del grupo de protocolos SPX/IPX de Novell.
- Interfaces NetBEUI de Microsoft.
- Protocolo de distribución de datagramas DDT (Datagram Delivery Protocol) de Apple Talk.

Protocolos del nivel de transporte.
Los protocolos de transporte permiten el intercambio de datos de extremo a extremo mediante el establecimiento de conexiones o sesiones inicialmente entre los sistemas para el intercambio para el intercambio secuencial y confiable de los datos. Algunos protocolos de transporte son:
- El protocolo de conexión de red avanzada APPN (Advanced Peer-to-peer Networking) de IBM.
- El protocolo para el servicio de transporte orientada la conexión COTS (Connection Oriented Transport Service) y servicios de transporte no orientados a la conexión CLTS (Connectionless Transport Services) de OSI.
- El protocolo de control de transmisión TCP (Transmisión Control Protocol) que es parte del grupo de protocolos TCP/IP de Internet y UNIX.
- Protocolo SPX que es parte de grupo de protocolos SPX/IPX de Novell.
- Interfaces NetBIOS y NetBEUI de Microsoft.
- Protocolo de encaminamiento de la tabla de encaminamiento RTMP, protocolo de eco AEP, Protocolo de transacción ATP, protocolos de vinculación de nombre NBP, todos de AppleTalk.

Protocolos de aplicación.
Los protocolos de aplicación permiten usar los servicios de comunicación de red y permiten la interacción entre las aplicaciones y permiten el intercambio de datos. Algunos ejemplos de protocolos de aplicaciones son:
- El protocolo de comunicación avanzada de programa a programa APPC de IBM.
- El protocolo para el acceso y gestión de la transferencia de archivos FTP.
- Protocolos para Internet como el sistema de archivos de red de Unix, el protocolo de transferencia de correo SMTP, Telnet, el protocolo básico de gestión de red SNMP.
- El protocolo principal de red NCP de Novell.

Los protocolos existen en cada nivel de las diferentes arquitecturas de los sistemas de comunicaciones para realizar alguna de las tareas que afectan a la comunicación entre los sistemas.

1.12 Medios de transmisión

El medio de transmisión es el sistema, sea físico o no, por el que viaja la información transmitida (datos, voz, video, audio, imágenes, etc.) entre dos o más puntos distantes entre sí. Por el medio viajan las señales electromagnéticas que son las que llevan la información.
Los medios de transmisión se dividen en dos grandes grupos:

1) Medios guiados o físicos. En los medios de transmisión guiados las señales circulan a través de un medio sólido o camino físico. Los medios físicos más usados son: el cable de par trenzado (UTP, STP, FTP), el cable coaxial, fibra óptica.
2) Medios no guiados o no físicos. En este tipo de medios de transmisión también llamados inalámbricos la señal ni se transmite ni se encauza por algún medio físico. Este medio puede ser el aire, el mar, el vacío o el espacio entre transmisor y receptor.

1) Medios de transmisión guiados

En este grupo de medio se produce un confinamiento de la señal y su capacidad de transmisión dependerá de:
- Distancia
- Tipo de enlace: Punto-a-Punto, difusión.

Los medios de transmisión guiados más usados son:

- El cable de par trenzado.
- El cable coaxial.
- La fibra óptica.

➢ El cable de par trenzado

El par trenzado es el medio físico o guiado mas barato y más usado. Consiste en un núcleo de hilos de cobre rodeados por un aislante (polietileno, PVC, etc.) que se encuentran trenzados por pares, de forma que cada par forma un circuito que puede transmitir datos, estos se trenzan con pasos diferentes para evitar acoplamientos de señal entre pares, el trenzado se realiza para evitar que se separen, para conseguir una impedancia bien característica (para asegurar una propagación uniforme de las señales de alta velocidad a lo largo del cable y para garantizar que la impedancia de los equipos que se conectan a la línea es la adecuada para que se transfiera la máxima potencia). Cuando se conoce la impedancia característica de una línea con precisión se puede diseñar una terminación adecuada que garantiza la no-reflexión de señales y por lo tanto que no haya errores, también se trenzan para incrementar la inmunidad frente a las interferencias electromagnéticas (interferencias y diafonía), las interferencias afectan ambos cables por igual, al cruzar los cables se reduce el crosstalk entre ellos así como el campo creado alrededor de los mismos con lo cual la corriente inducida alrededor de cada uno se ve cancelada por la corriente de retorno del otro.
Los hilos empleados son de cobre sólido de 0.2-0.4 mm de diámetro. El paso de torsión de cada cable puede variar entre una torsión por cada 7 cm para los de peor calidad y 2 vueltas por cm en los de mejor calidad.
Existen dos tipos cable de par trenzado muy utilizados:

- El cable de par trenzado UTP.
- El cable de par trenzado STP.

- **Cable de par trenzado UTP.**

El cable de par trenzado sin apantallar UTP (Unshielded Twisted Pair) es el mas conocido al ser una tecnología barata y sencilla de instalar, pero es menos resistente a interferencias tanto exteriores como procedentes de pares adyacentes, por su flexibilidad es muy usado en telefonía y redes de área local. Su impedancia característica es de 100 ohms. Sus limitantes son: es resistente al flujo de electrones lo que limita la distancia de transmisión, produce radiación de energía en forma de señales que se pueden detectar, además de ser sensible a la radiación externa que produce distorsión sobre la transmisión.

La norma EIA/TIA 568 lo divide en varias categorías destacando las siguientes:

- Categoría 3. En la cual la velocidad de transmisión es de 16 Mhz a 100 m de distancia máxima.
- Categoría 5. Maneja una velocidad de 100 MHZ a 100 m de distancia máxima. Esta es la mas usada actualmente, aunque ya existen otras categorías como la 5e e incluso la categoría 6.

- **Cable de par trenzado STP.**

En el cable de par trenzado apantallado STP (Shielded Twisted Pair) cada par es envuelto por una malla metálica y a su vez el conjunto de pares de alambres que forman el cable se recubre por otra malla lo que forma una jaula de Faraday, esto para ser más resistente a las interferencias, a la diafonía y la atenuación. Aunque permiten mejores ancho de banda y mayor velocidad de transmisión, el enmallado incrementa su costo y son un poco más difíciles de instalar ya que son más gruesos y rígidos que el UTP. El STP estandarizado por EIA/TIA 568 es un cable de impedancia característica de 50 ohms que trabaja a una frecuencia de 300 Mhz, usa conectores RJ45 metálico y hermafrodita.

El cable de par trenzado es un medio de transmisión de bajo costo que puede transmitir señales analógicas y digitales es muy utilizado en redes de área local a 10, 100 y 1000 Mbps, también se usa en la transmisión analógica como la telefonía para conectar la parte del bucle del abonado a las centrales locales, en la transmisión digital como RDSI. El STP se ha usado también para enlaces de comunicaciones que usan técnicas de multiplexación en el tiempo funcionando a velocidades de 1,544 Mbps y 2,048 Mbps permitiendo una distancia entre repetidores de aproximadamente 1.5 Km.

Debido a que las señales de alta frecuencia circulan por la superficie exterior de los conductores, los cables de pares trenzados resultan ineficientes, ya que esas corrientes de superficie provocan que la atenuación se incremente con la raíz cuadrada de la frecuencia.

- **El cable coaxial**

El cable coaxial consiste de dos conductores cilíndricos concéntricos, un cable conductor interno cilíndrico de cobre sólido separado de otro cable conductor externo por anillos aislantes que forman una especie de pantalla y cable de tierra, la funcionalidad de este conductor externo es hacer que el cable coaxial sea muy poco sensible a interferencias y diafonía, el material eléctrico entre los conductores es un material dieléctrico (polietileno, PVC). Todo esto se recubre por otra capa aislante que es la funda del cable.

Este medio es mas caro que el par trenzado pero se puede para distancias más largas, con mayores anchos de banda y velocidades transmisión superiores aunque actualmente las técnicas del par trenzado ya igualan las velocidades de este, es menos susceptible a interferencias y permite conectar mas equipos. El ancho de banda que se puede obtener

esta en función de la distancia, para cables de 1 Km se puede llegar a velocidades de hasta 10 Mbps y en cables de longitud menores la velocidad es incluso mayor que esta. Su respuesta en frecuencia es de hasta 400 MHz, superior a la de par trenzado, sus limitantes son el ruido térmico, ruido de intermodulación, necesita amplificadores mas frecuentemente que el par trenzado, puede ser rígido o flexible. Las interferencias eléctricas no tienen importancia si la pantalla exterior carece de discontinuidades. El uso de portadoras de alta frecuencia hace inmune al sistema frente a interferencias de baja frecuencia originadas por dispositivos eléctricos y otras fuentes electromagnéticas.
Por su impedancia hay dos clases de cable coaxial:

- Cable coaxial de banda base que tiene una impedancia de 50 ohms y se usa para transmisión digital.
- El cable coaxial de banda ancha con una impedancia de 75 ohms para transmisiones analógicas.

Por su tipo de aislante existen tres clasificaciones básicas de estos cables:

- Cable coaxial estándar del tipo RG. Usan polietileno como aislante interior aunque algunos usan aire. Los de 1 cm de diámetro manejan velocidades hasta de 30 Mbps.
- Núcleo aislado por aire, es de diámetro pequeño, es retardador para caso de incendio, tiene una constante dieléctrica pequeña por lo que sus propiedades eléctricas son mejores que las del tipo RG. Tiene una atenuación baja, 400 dB/100, a 400MHz para los de malla trenzada y 50 dB para los de malla continua.
- De polietileno celular irradiado son mas caros que los de aire pero no presentan las variaciones de aquellos al ser doblados.

El cable coaxial suele utilizarse como cable de antena de TV, para transmisión de televisión, telefonía a larga distancia entre centrales, en redes de área local, anteriormente era el medio más usual para redes ethernet y ARCNET, también se emplea para enlaces entre centrales telefónicas que utilizan técnicas TDM. Transmite señales analógicas para lo cual necesita un amplificador cada pocos kilómetros o digitales con un repetidor cada kilómetro.

- **La fibra óptica**

La fibra óptica es un medio muy flexible y muy fino que conduce energía de naturaleza óptica (luz). Usa los pasos de luz para transmitir las señales digitales, así un pulso de luz representa al 1 binario y la ausencia del pulso de luz representa al 0 binario. La transmisión de señales luminosas (fotones) es a través de un núcleo de dióxido de silicio puro. Su forma es cilíndrica con tres secciones: núcleo, revestimiento y cubierta. El diámetro de la cubierta es de unas centenas de μm (típicamente 125 μm), el núcleo se formas de varias fibras muy finas de cristal o platico suele medir entre 2 y 10 μm.
Los núcleos pueden ser de vidrio o de platico (polímero). El de plástico es más flexible y los conectores se adaptan mejor sin necesidad de pulir los extremos, tienen mayor diámetro en el núcleo, es menos sensible a impurezas, es mas barato que el vidrio pero su atenuación es mayor lo que limita la longitud del enlace.
Cada fibra esta rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Este conglomerado esta rodeado de la cubierta que lo protege de aplastamientos, humedad, mide decenas de mm. Las fibras ópticas no son afectadas por la radiación exterior a la vez que su forma de transmisión fotonica no produce emisiones externas al cable.
La transmisión por fibra óptica se basa en la diferencia de índice de refracción entre el núcleo y la cubierta que tiene un índice de refracción menor. El núcleo transmite la luz

y el cambio que experimenta el índice de refracción en la superficie de separación provoca la reflexión total de la luz, de forma que solo abandona la fibra una mínima parte de la luz transmitida. Dependiendo del cambio de valor del índice de refracción las fibras ópticas se dividen en:

- Fibras ópticas de índice a escala donde el cambio es muy abrupto.
- Fibras ópticas de modo gradual que experimentan un cambio gradual parabólico.

Como ya hemos mencionado su método de transmisión es mediante rayos de luz que inciden con una gama de ángulos diferentes posibles en el núcleo del cable, solo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo, sobre la base de estos ángulos puede tener dos formas de transmisión:

- Transmisión Multimodal de índice de escala en la cual llegan a su destino los rayos que inciden en un cierto rango de ángulos para poder ir rebotando a lo largo del cable. Su inconveniente es que dependiendo del ángulo de incidencia de los rayos estos toman trayectorias diferentes y tardan mas o menos tiempo en llegar al destino provocando distorsión y limitación de la velocidad de transmisión posible debido a la dispersión de los componentes. El diámetro del núcleo esta entre los 50 y 60 μm pero puede llegar a los 200 μm, el del recubrimiento se acerca al estándar de los 125 μm. Sus aplicaciones se limitan a transmisión de datos de baja velocidad o cables industriales de control.
- Transmisión Multimodo de índice gradual, el diámetro del núcleo esta entre 50 y 60 μm y el recubrimiento es de 125 μm, se cambia el índice de refracción del núcleo para reducir la dispersión y así aumentar la velocidad.
- Transmisión Monomodal en la cual se reduce el radio del núcleo (entre 1 y 10 μm), recubrimiento de 125 μm de diámetro, por lo que el rango de ángulos diminuye hasta que solo se transmite un rayo, el rayo axial. La luz recorre una única trayectoria, proporcionando un gran ancho de banda. Como la dispersión es baja se consiguen anchos de banda de varios GHz/Km.

Las longitudes de onda de los haces de luz producidos en la fibra óptica se encuentran en el rango de 10^{14}-10^{15} μm por lo que su rango de frecuencias de transmisión es todo el espectro luz visible y parte del infrarrojo.

Para realizar la transmisión de información un diodo emisor de luz LED situado en un extremo emite destellos (representan al 1 y al 0 lógicos) que se transmiten por el cable de fibra hasta el otro extremo donde se recogen por un fotodetector y se convierten en señales eléctricas. Puesto que no existe una resistencia a las señales transmitidas, la velocidad de transmisión por fibra óptica supera ampliamente a la transmisión por cobre.

Para la emisión de la luz se usan LED´s de bajo costo y utilización en un amplio rango de temperaturas y los diodos láser que son mas caros, pero más eficaces y permiten una mayor velocidad de transmisión a mayor distancia.

La fibra óptica es muy medio muy apropiado para largas distancias, e incluso para redes Lan. Sus ventajas frente a cables coaxiales y pares trenzados son:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz ($c=3x19^9$m/s), mientras que en las señales eléctricas la velocidad es el 50 u 80% de esta velocidad. Pueden lograrse velocidades de varios Gbps a decenas de Km sin necesidad de repetidor. Cuanto mayor sea la longitud de onda, mayor será la distancia y la velocidad de transmisión.
- Por la alta frecuencia de transmisión se tiene un ancho de banda enorme.
- Aislamiento electromagnético. Gracias a su estructura y funcionamiento tienen una gran inmunidad a interferencias electromagnéticas incluidos los pulsos electromagnéticos nucleares.

- Menores tasas de error que en cable coaxial lo que aumenta la velocidad eficaz de transmisión al reducir las retransmisiones o cantidad de información redundante para detectar y corregir errores de transmisión.
- Menor peso y tamaño.
- Menor atenuación
- Permite una mayor distancia entre repetidores.
- Es un medio difícil de manipular
- Tiene una alta seguridad
- Soporta una alta gama de temperaturas
- Mayor resistencia a ambientes líquidos y corrosivos que los cables eléctricos.

Una desventaja de este medio es que es un medio difícil de manipular y por lo tanto difícil de reparar en caso de daño.
Por sus capacidades se puede aplicar en:
- Transmisiones a larga distancia para telefonía, una fibra puede contener 60000 canales.
- Transmisión metropolitana para enlaces cortos en entornos de 10 Km, sin necesidad de repetidores y con capacidad de 100,000 conversaciones por cada fibra.
- Acceso a áreas rurales para cubrir longitudes de 50 a 150 Km, con un transporte de 5000 conversaciones por fibra.
- Bucles de abonado
- Redes de área local de alta velocidad.

2) Medios de transmisión no guiados.

El medio de transmisión no guiado más usado es el aire. Para fines de los sistemas de comunicaciones la transmisión por medio del aire se puede realizar a diferentes frecuencias por lo que tenemos los siguientes tipos de transmisión por frecuencia o por tipos de ondas del espectro electromagnético:

- Transmisión con ondas de radio frecuencia. Para enlaces con varios receptores, usan bajas frecuencias. Son ondas omnidireccionales para transmisión en el rango de frecuencias de 10Mhz a 1 GHz.
- Transmisión con microondas terrestres. Para enlaces punto a punto, usan altas frecuencia. Son ondas direccionales para comunicaciones terrestres en el rango de frecuencias de 2 GHz a 40 GHz.
- Transmisión con microondas por satélite. Para enlaces punto a punto usan altas frecuencias. Son ondas direccionales para comunicaciones por satélite en el rango de frecuencias de 2 GHz a 40 GHz.
- Transmisión con infrarrojos. Usados para transmisiones a muy corta distancia, por ejemplo, dentro de una habitación. Usados para la comunicación en el rango de frecuencias de $3x10^{11}$-20 THz.

Cada uno de estos tipos de transmisión usa un rango de frecuencias del espectro electromagnético. El espectro de frecuencias de transmisión se divide en bandas como muestra la tabla 1.12.1

Abreviatura	Nombre	Frecuencia
VLF	Muy Baja (Very Low Frequency)	3-30KHz
LF	Baja (Low Frequency)	30-300KHz
MF	Media (Mid Frequency)	300-3000KHz
HF	Alta (High Frequency)	3-30MHz
VHF	Muy Alta (Very High Frequency)	30-300MHz
UHF	Ultra alta (Ultra High Frequency)	300-3000MHz
SHF	Super Alta (Super High Frequency)	3-30GHz
EHF	Extra Alta (Extra High Frequency)	30-300GHz
		300-3000GHz

Tabla 1.12.1 Bandas de transmisión del espectro de frecuencias

- **Transmisión con ondas de radio frecuencia**

La radiocomunicación utiliza el aire para la comunicación por medio de ondas radioeléctricas también conocidas como ondas de radio.

Ondas de radio

Las ondas se radio son omnidireccionales, por lo que no se necesitan antenas parabólicas, utilizan la banda entre 30MHz-1GHz para transmitir señales de FM, TV (UHF, VHF), datos.

Las ondas radioeléctricas son ondas electromagnéticas que se propagan por el espacio sin guía artificial, el limite superior de frecuencia del espacio se fija convencionalmente en 3,000 GHz. Este medio de transmisión se usa como una forma de evitar tender un cableado en áreas donde no es posible usar medios guiados.

La técnica de radiocomunicación consiste en la superposición de la información que se desea transmitir en una onda portadora electromagnética mediante la modulación. La onda modulada se envía al medio de propagación a través de un dispositivo de acoplamiento con el medio denominado antena. La antena radia energía electromagnética, energía que es captada con otra antena. Cuando la onda transmitida alcanza el punto de destino accede al sistema de recepción por medio de una antena de recepción que capta una fracción de la energía. El alcance útil o cobertura de una emisión radioeléctrica depende del tipo e intensidad de las perturbaciones.

La transmisión por radio puede ser de dos tipos:

- Omnidireccional. La antena transmisora emite la energía que se dispersa en múltiples direcciones espaciales por lo que varias antenas pueden captarla igualmente en cualquier dirección. La transmisión se realiza mediante señales de baja frecuencia.
- Direccional. Toda la energía se concentra en un haz que es emitido en una cierta dirección por lo que tanto el emisor como el receptor deben estar alineados, cuanto mayor es la frecuencia a transmitir más factible es la transmisión unidireccional.

Las perturbaciones en este tipo de comunicaciones son provocadas por reflexiones tanto en tierra como en mar.

La radio comunicación que usa elementos situados en el espacio se conoce como radiocomunicación espacial, cualquier otra se conoce como radiocomunicación terrestre.

➢ **Transmisión con microondas terrestres**

Las microondas son una porción del espectro electromagnético de frecuencias, y a su vez el espectro de frecuencias de las microondas presenta una división en bandas como muestra La tabla 1.12.2

Banda	Frecuencias
L	1-2GHz
S	2-4GHz
C	4-8GHz
X	8-12GHz
Ku	12-18GHz
K	18-27GHz
Ka	27-40GHz

Tabla 1.12.2 Espectro de microondas

Para la transmisión con microondas terrestres suele usarse antenas parabólicas de tres metros de diámetro, sustituyen al cable coaxial y fibra óptica ya que se necesitan menos repetidores y amplificadores aunque se necesitan antenas alineadas debido a que el haz es muy estrecho. Para que esquiven mejor los obstáculos y alcancen una distancia mayor deben estar a la mayor altura que se pueda.

Se pueden usar para la transmisión de televisión y voz ya que el ancho de banda y la velocidad de transmisión aumenta con la frecuencia como muestra la tabla 1.12.3, transmisión a larga distancia ya que requiere menos repetidores que el cable coaxial.

Banda (GHz)	Ancho de Banda (MHz)	Régimen de transmisión (Mbps)
2	7	12
6	30	90
11	40	90
18	220	274

Tabla 1.12.3 ancho de banda y velocidad de transmisión de microondas

Su principal causa de perdidas es la atenuación la cual aumenta con el cuadrado de la distancia y las lluvias. Si hay muchos sistemas de microondas también se pueden causar interferencia debido al traslapamiento de señales por lo que tiene que haber una regulación de las bandas como muestra la tabla 1.12.4.

4-6 (GHz)	Transmisión a larga distancia
12 GHz	Directos
22 GHz	Televisión por cable

Tabla 1.12.4 Bandas de transmisión para los sistemas de microondas

Se pueden aplicar en enlaces punto-a-punto sobre distancias cortas como circuitos cerrados de televisión, interconexión de redes locales y transmisión entre edificios.

- **Transmisión con microondas por satélite**

En este tipo de transmisión un satélite actuando como estación repetidora recibe la señal de la antena transmisora y la amplifica, la regenera o la retransmite en la dirección adecuada hacia varias estaciones terrestres receptoras, este satélite debe ser geoestacionario para estar alineado con los receptores y emisores de la tierra. Su rango de frecuencias de transmisión es diferente al de recepción para que no se interfieran las señales que ascienden con las que descienden, tabla 1.12.5.

Ascendente (GHz)	Descendente (GHz)	Ancho de banda (MHz)
4	6	500
12	14	500
19	29	2500

Tabla 1.12.5 Frecuencias de ascenso y descenso

Para evitar interferencias entre satélites por norma debe de haber una separación entre ellos de 3° (para la banda de 12-14GHz) o 4°(Para la banda de 4-6 GHz). La banda de operación de cada satélite se conoce como transpondedor.
El rango de frecuencias satelital optimo es de 1-10GHz. Ya que por debajo de 1GHz el ruido solar, galáctico y atmosférico causan problemas. Arriba de 10GHz la absorción atmosférica y la atenuación por lluvia tienen mucha predominancia.
Se debe de tener especial control de errores y flujo de la señal debido al retardo provocado por las largas distancias que recorre la señal desde que es emitida en la tierra hasta que es devuelta al receptor.
Este sistema puede usarse para difusión de televisión, proporciona enlaces punto-a-punto para transmisión telefónica de larga distancia internacional. Redes privadas, para lo cual la capacidad del canal de comunicaciones es dividida en diferentes canales de menor capacidad que se alquilan a empresas privadas, las cuales crean su propia red sin necesidad de poner un satélite en orbita.

- **Transmisión por Infrarrojos**

En un sistema de transmisión por rayos infrarrojos los emisores y receptores de infrarrojos deben estar alineados o estar en línea tras la posible reflexión del rayo en superficies como las paredes, por lo tanto hacen uso de la reflexión directa. Este tipo de medio de transmisión no tiene problemas de seguridad ni interferencias ya que por ejemplo no atraviesan las paredes ni algún otro obstáculo. Además no es necesario un permiso para su uso como en el caso de las microondas y ondas de radio en las cuales se necesita un permiso par asignar una frecuencia de uso.
No se pueden establecer enlaces en medios abiertos debido al cambio de las condiciones climatologicas que actúan como obstáculos.

2. MODELO DE REFERENCIA OSI Y TIPOS DE REDES

2.1 Organismos de estandarización.

Debido a la gran variedad de productos y equipos derivados del desarrollo y avance de la tecnología en diferentes áreas, en este caso el de las telecomunicaciones, se hace necesario normar la fabricación y funcionamiento de los mismos.
La estandarización o normalización se vuelve una necesidad a partir de que los fabricantes crean sus propios equipos y protocolos propietarios, lo cual representaba un problema grave para el usuario final que no puede interconectar los equipos de un fabricante con los de otro en su red.
La normalización permite que diferentes compañías fabriquen equipos compatibles y complementarios lo facilita la comunicación e interoperabilidad entre equipos diferentes a la vez que incrementa el uso y adquisición de equipos apegados a las normas.
Un proceso de normalización o estandarización es resultado del consenso de todos o la mayoría de los implicados en una determinada área sobre las especificaciones y criterios a aplicar de manera consistente en la elección y clasificación de los materiales, procesos de fabricación y provisión de servicios.
Los objetivos de establecer una normalización son entre otros: mejorar la calidad de los productos a un precio razonable, mayor compatibilidad e interoperabilidad de los bienes y servicios, simplificación de uso, reducción del número de modelos y costos, así como el aumento de la eficacia de la distribución y facilidad de mantenimiento.
Los procesos de normalización dan como resultados la promulgación de estándares.
Los estándares son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para su utilización como normas, guías o definición de características con el objetivo de asegurar que los materiales productos, procesos y servicios se ajustan a su propósito.
Por su ámbito de aplicación los estándares se pueden clasificar como: estándares de organizaciones profesionales representativas de la industria como los de la IEEE, estándares de gobierno MAP, estándares multifabricantes como los de ECMA, estándares nacionales como ANSI, estándares multinacionales (CEN) y estándares internacionales como los de ISO.
Los estándares por su nivel de obligatoriedad se clasifican como:

- No vinculantes en los que no hay obligación alguna de adherirse.
- Obligatorios y no obligatorios sectorial. Para cuando las ventas de un producto al gobierno se limita para aquellos que satisfacen los estándares.
- Estándares de jure (de derecho o ley) Son estándares formales, legales que se adoptan por un organismo que se encarga de normalizar, por lo que se conocen también como estándares oficiales. Son los promulgados por asociaciones reconocidas oficialmente como los protocolos ISO, X25 o ATM.
  Pero dentro de estos tenemos a los extraoficiales que son declarados por miembros de los organismos oficiales como sucedió con el ATM-forum, Internet Society.
- De facto (de hecho). También llamados estándares de la industria, son estándares que se establecieron sin algún planteamiento formal. Son los de aceptación general por los usuarios aunque hayan sido definidos por un solo fabricante, o han sido

aceptados por un significativo numero de fabricantes y grupos de usuarios como sucedió con (TCP/IP).

Los organismos de estandarización están dedicados al establecimiento de normas o estándares, algunos de estos organismos se observan en la Fig. 2.1.1

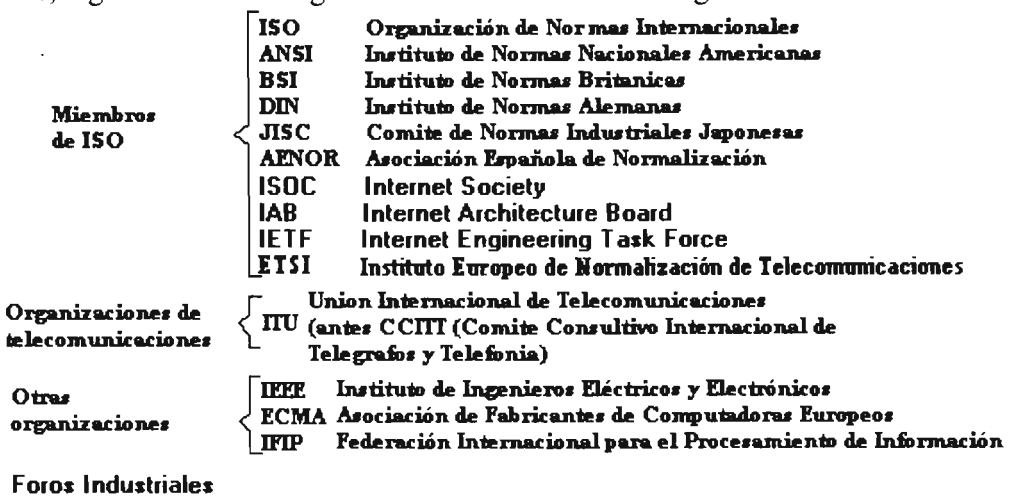


Fig.2.1.1 Organismos de Estandarización

Los organismos de normalización de la Fig. 2.1.1 la mayoría no se dedican exclusivamente al área de comunicaciones a excepción de la ITU que esta constituido por los operadores de las telecomunicaciones. A continuación se describen brevemente las funciones de algunos de ellos.

ISO

La Organización Internacional para la Estandarización (ISO) es la organización no gubernamental en el ámbito mundial que coordina el desarrollo y aprobación de los estándares como estándares internacionales.

Su misión es promover el desarrollo de la estandarización y actividades relacionadas en todo el mundo con el objetivo de facilitar el intercambio de bienes y servicios y la cooperación en los ámbitos intelectuales, científicos, tecnológicos y económicos.

Su ámbito de trabajo cubre todas las áreas que van la estandarización de lenguajes de programación y protocolos hasta normas para pasos de rosca de tuercas y tornillos, números ISBN, tamaño de papel, recubrimientos de cables telefónicos, incluyendo la normalización de las redes de área local, etc. Se constituye por organizaciones nacionales de los principales países desarrollados, por ejemplo ANSI que representa a EU.

Su organización es de forma jerárquica:

- El trabajo de ISO se estructura en un gran número de comités técnicos (TC Technical Comitee), cada uno responsable de una determinada área de la tecnología.
- Dentro de cada comité existen subcomités (SC) con responsabilidades especificas
- Y a su vez cada uno de los subcomités se divide en grupos de trabajo (WG) que colaboran con la elaboración de propuestas de estandarización.

Uno de los principales trabajos de ISO ha sido el establecimiento del modelo de referencia OSI. Algunos estándares de ISO en comunicaciones son:

- ISO 7498 El modelo OSI.
- ISO 3309 HDLC (protocolo a nivel de enlace).
- ISO 8802.3 El estándar IEEE 802.3 (Ethernet).
- ISO 8801 Normativa de cableado estructurado.
- ISO 8473 CLNP Conectionless Network Protocol (variante de IP hecha por OSI).

IEEE

Por su parte el IEEE es una organización profesional, realizó las primeras tareas de normalización en el ámbito de las redes de área local, cuyos proyectos 802.x ofrecen directrices orientadas a guiar la fabricación de componentes y software para las redes de área local que han sido adoptadas como estándares de facto en la industria. Estos proyectos IEEE802.x se adoptan como estándares internacionales por ISO 8802.x.

ANSI

El organismo de estandarización americano ANSI coordina y sincroniza las actividades de otras organizaciones que desarrollan estándares y se asegura que todos los intereses afectados tengan oportunidad de participar en el proceso. Es el representante de EU en la ISO, se constituye de fabricantes, proveedores de servicios portadores comunes y otros grupos interesados. Las normas de ANSI frecuentemente son aceptadas por la ISO como normas internacionales de facto.

ITU

La Union Internacional de Telecomunicaciopnes (ITU) es una organización mundial perteneciente a la ONU en la cual participan gobiernos y sector privado como operadoras, fabricantes de equipos, organizaciones científicas, bancos, etc. Los cuales coordinan el establecimiento y operación de los servicios y redes de telecomunicaciones. Es el responsable de la regulación, normalización, coordinación y desarrollo de las telecomunicaciones internacionales. Su objetivo es facilitar el desarrollo de las telecomunicaciones para el beneficio universal de la humanidad mediante la definición de recomendaciones y cooperación mutua, sus recomendaciones no son obligatorias.

La ITU tiene sus orígenes en varios comités consultivos internacionales entre ellos el CCITT que desaparecieron para dar origen a esta.

El crecimiento exponencial de las telecomunicaciones enfrenta a la ITU con nuevos problemas y tendencias como la globalización, la desregularización, la reestructuración, redes de servicios de valor agregado, redes inteligentes, convergencia de servicios y tecnología, entre otros, con lo cual su trabajo cada vez es más complejo. Para poder cubrir toda esta amplia gama de áreas de normalización la ITU ha sido dividida en los sectores ITU-R (Sector de Radiotelecomunicaciones), ITU-T (Sector de Normalización de Telecomunicaciones) y el sector de desarrollo de telecomunicaciones.

ITU-T analiza las cuestiones técnicas de operación y tarificación y emite recomendaciones sobre las mismas con el objetivo de tener una normalización de ámbito global. Sus actividades cubren aspectos como la operación de red y servicios, tarificación, mantenimiento, comunicación de datos, conmutación, señalización, lenguajes hombre-maquina y RDSI (Redes Digitales de Servicios Integrados). Produce estándares relacionados con el acceso a las redes publicas por lo cual a tenido muy poca influencia en las redes de área local a pesar de ser una organización importante en la normalización de telefonía y redes de datos.

El trabajo en ITU-T es realizado por grupos de estudio, tabla 2.1.1, los cuales desarrollan las recomendaciones que son publicadas en los libros de colores.

Grupo de estudio 1	Definición de Servicios
Grupo de estudio 2	Operación de Red
Grupo de estudio 3	Principios de costos y tarificación
Grupo de estudio 4	Mantenimiento de Red
Grupo de estudio 5	Protección contra efectos de ambientes electromagnéticos
Grupo de estudio 6	Planta exterior
Grupo de estudio 7	Redes de Datos y Comunicaciones de Sistemas Abiertos
Grupo de estudio 8	Terminales para servicios telemáticos
Grupo de estudio 9	Transmisión de televisión y sonido
Grupo de estudio 10	Lenguajes para aplicaciones de telecomunicaciones
Grupo de estudio 11	Conmutación y señalización
Grupo de estudio 12	Desempeño de la transmisión de extremo-a-extremo de redes y terminales
Grupo de estudio 13	Aspectos generales de redes
Grupo de estudio 14	Modems y técnicas de transmisión para datos, telégrafos y servicios telemáticos
Grupo de estudio 15	Equipos y sistemas de transmisión

Tabla 2.1.1 Grupos de estudio de normalización ITU

Al igual que la ISO tiene una división jerárquica por lo que los grupos de estudio se dividen en Working Parties que a su vez se dividen en Expert Teams.
Las recomendaciones de la ITU-T se identifican por una letra que indica el tema de la serie de recomendaciones seguida por un número, algunos ejemplos de estas letras son:

- E- redes telefónicas y RDSI.
- V- comunicación digital sobre la red telefónica.
- X- redes públicas de comunicación de datos.
- I- RDSI.
- Q- Operación y mantenimiento.

Como ejemplo de algunos estándares de La ITU tenemos:

- X.25 Red pública de conmutación de paquetes.

- X.400 Sistema de mensajeria de correo electrónico.
- V.35 Interfaz de nivel físico para líneas punto a punto.
- V.90 Modems de 56/33.6 kbps.
- H.323 Videoconferencia sobre IP (Netmeeting).
- G.711 Digitalización de la voz en telefonía.
- G.957 Interfaz óptica de equipos SDH.
- G.DMT ADSL.

ETSI

En el ámbito europeo tenemos al Instituto Europeo de Normalización de Telecomunicaciones (ETSI), cuyo objetivo principal es la estandarización de las telecomunicaciones europeas unificadas. Se compone de administraciones y organizaciones de normalización nacionales, operadores de redes públicas, usuarios, fabricantes, proveedores de servicios. Se divide en comités técnicos dedicados a aspectos de red, sistemas y equipamiento de radio y comunicaciones móviles. Uno de sus éxitos fue la finalización del Sistema Global para Comunicaciones Móviles GSM, sistema celular único para toda Europa. Dentro de las organizaciones de estandarización europeas también tenemos el CEN (Comité Europeo de Estandarización) y el CENELEC (Comité Europeo de Estandarización electrotécnica). Los estándares creados por estos últimos se denominan normas europeas mientras los del ETSI son estándares europeos (EN) de telecomunicación (ETSs).

IAB

Por el gran crecimiento de Internet es importante destacar al IAB (Internet Activities Board) que se desenvuelve en el ámbito de los estándares "de facto", es el responsable de la definición de los estándares de hecho en la comunidad Internet. Define y desarrolla los estándares conocidos genéricamente como TCP/IP. Las recomendaciones para nuevos protocolos o mejoras de protocolos se emiten a través de documentos denominados RFC (Request for Comment), estos RFC se asignan a un grupo de trabajo de IETF (Internet Engineering Task Force).

Los RFC se clasifican como mandatorios (requeridos), recomendados, electivos, de uso limitado y no recomendado.

Cuando se demuestra que los protocolos funcionan correctamente y son aceptados por los usuarios se convierten de manera natural en estándares de facto.

Foros industriales.

Los foros industriales son grupos interesados en la estandarización de una tecnología por lo que se integran con fabricantes, operadores de telecomunicaciones, universidades, etc. Nacen como una presión hacia los organismos oficiales como ISO e ITU por la lentitud con que aprueban los estándares internacionales, por lo que ponen fechas límite para la adopción de sus resoluciones. Algunos ejemplos de estos foros son:

- El ATM Forum.
- El Frame Relay Forum.
- El Gigabit Ethernet forum.
- El ADSL forum.
- EL IPV6 forum.

2.2 Concepto del Modelo OSI

El modelo de referencia OSI (Open System Interconection=Sistema de Interconexión Abierto) es un estándar internacional que establece las bases para la normalización y definición de protocolos de comunicación entre sistemas de telecomunicaciones e informaticos.
Su principal objetivo es la interconexión de sistemas de diferentes fabricantes es decir la Interconexión de Sistemas Abiertos. Es un modelo de referencia para los fabricantes ya que les proporciona un conjunto de estándares que aseguran la compatibilidad entre los distintos tipos de tecnología de red utilizados por las empresas en el ámbito mundial.
El propósito general del modelo es identificar áreas de desarrollo o mejora de estándares y proporcionar una referencia común para el mantenimiento de los mismos. Es un marco conceptual y funcional que permite a los equipos internacionales trabajar de manera productiva e independiente en el desarrollo de estándares para cada nivel del Modelo de Referencia OSI.
La idea del modelo de referencia es manejar la comunicación sobre la base de módulos, ya que el diseño e implementación de cada modulo es más manejable mediante la división de los mismos en tareas más pequeñas y concretas. Aunado a esto el mantenimiento y la modificación es más eficiente ya que cada nivel puede ser reemplazado sin alteración de los niveles adyacentes.
Los causas de la definición del sistema ISO se encuentran en el diseño de bases de datos distribuidas y el aumento en el uso de las redes que hicieron necesaria una arquitectura de comunicaciones estructurada y distribuida. El análisis de los sistemas SNA de IBM y ARPANET dio lugar a una arquitectura de 7 niveles conocida como arquitectura de sistemas distribuidos.
El comité de sistemas abiertos de ISO eligió la arquitectura por niveles con la condición de que esta cumpliera con la mayoría de los requerimientos exigibles para la interconexión de sistemas abiertos así como el reconocimiento de la capacidad de expansión del modelo para adecuarse a requerimientos futuros.
Para poder simplificar el estudio e implementación de la arquitectura de red, la ISO dividió el modelo de referencia OSI en capas. Una capa es una entidad que realiza una función específica.
En base a este modelo cada sistema abierto esta lógicamente formado por un conjunto ordenado de subsistemas, concretamente son 7 subsistemas, niveles o capas:

- Capa física
- Capa de enlace
- Capa de red
- Capa de transporte
- Capa de sesión
- Capa de presentación
- Capa de aplicación

Estos niveles junto con el medio físico proporcionan un conjunto completo de servicios de comunicación, Fig. 2.2.1.

Fig. 2.2.1 Modelo OSI y sus niveles

Cada capa define los procedimientos y reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir para poder comunicarse con los procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de la capa OSI. Las tres capas superiores de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos.
Las ventajas de tener un modelo de referencia en capas o niveles son las siguientes:
- Todo un sistema complejo es simplificado por los subsistemas que lo componen.
- Las interfaces son estándares.
- La ingeniería es modular, lo cual impide que los cambios en una capa puedan afectar a las demás capas, esto permite a su vez que se puedan desarrollar con mas rapidez.
- Se tiene la certeza de que el sistema puede interoperar con otros distintos, siempre y cuando estén también estandarizados.
- Se acelera la evolución.
- Divide la comunicación en red en partes más pequeñas para simplificar el aprendizaje.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.

Cada nivel tiene una función que se define con los servicios OSI.
La comunicación entre niveles de sistemas diferentes se realiza mediante la definición y uso de un lenguaje mas conocido como protocolo, para poder hablar y entenderse con su pareja en el otro extremo, este protocolo es independiente de los protocolos de los demás niveles.
El modelo tiene tres niveles de abstracción:

- Arquitectura OSI. Define los elementos básicos de los sistemas abiertos abstractos, es decir la manera en que debe verse un sistema desde el exterior.

- Especificaciones de servicio OSI. Las especificaciones definen los servicios proporcionados a los usuarios en cada nivel, es decir los servicios proporcionados por un nivel al nivel superior.
- Especificaciones de protocolos OSI. Definen la información de control transmitida entre los distintos sistemas, así como los procedimientos para la interpretación de dicha información de control.

El conjunto de funciones del sistema es dividido en niveles para facilitar su estudio y desarrollo, para que sean controlables de forma individual y que en conjunto resuelvan las necesidades de comunicación. Cada nivel se desarrolla sobre el anterior, de modo que recibe una serie de servicios sin conocer los detalles de cómo se realizan dichos servicios.
Las diferentes funciones de la arquitectura OSI se estructuran en los 7 niveles, la función de cada uno es complementaria. La Fig.2.2.2 muestra la arquitectura de una red usando el modelo OSI

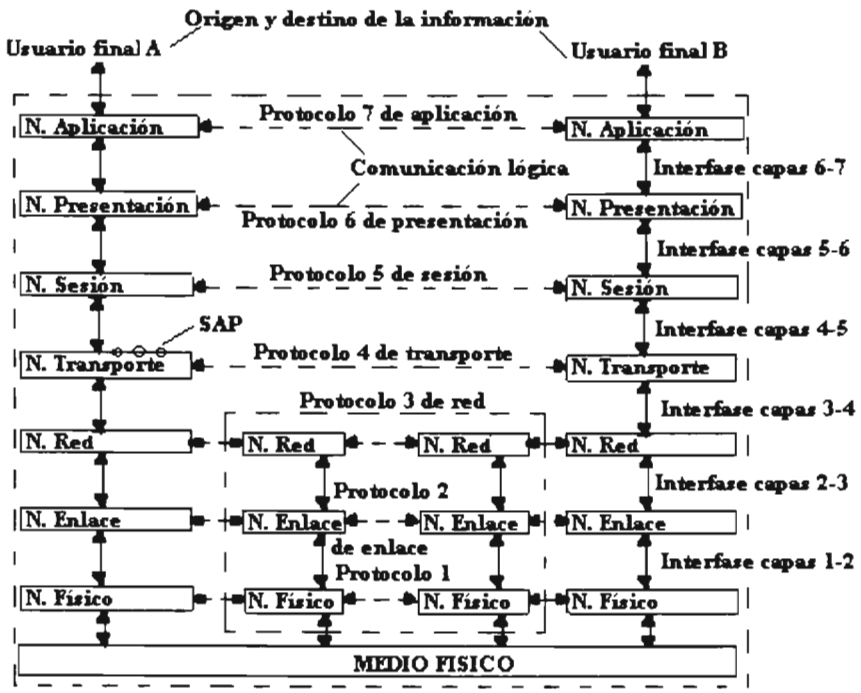


Fig. 2.2.2 Arquitectura de una red basada en el modelo OSI

- La estructura de la red se compone de nodos que pueden ser un sistema central, una unidad de control de comunicaciones o una terminal.
- En el modelo el usuario final es el origen o receptor de la información el cual puede ser una aplicación o un dispositivo de entrada / salida.
- El nivel es cada una de las particiones del sistema. El nivel n de un extremo conversa con el nivel n del otro extremo. Son los procesos pares los que se comunican mediante el uso del protocolo.

No existe una transferencia directa de la capa n de un extremo a la capa n del otro.
La unidad funcional o entidad es un proceso activo que se ejecuta dentro de un mismo nivel e implementa funciones y servicios de ese nivel para ofrecerlos al nivel superior. Pueden

existir distintas unidades de las cuales cada una de ellas implementa funciones diferentes como protocolos distintos.
Cada nivel se relaciona con el nivel inmediatamente superior e inferior a través del concepto de interfaz. La interfaz representa el conjunto de elementos lógicos (formados por el conjunto de reglas que gobiernan el intercambio de información por un SAP) y físicos existentes entre dos niveles adyacentes.
Los procesos que una unidad realiza y cuyos resultados son ofrecidos o empleados por el nivel superior son los servicios de nivel proporcionados a través de los puntos de acceso al servicio (SAP, Service Access Point) de la interfaz.
Las unidades de datos intercambiadas por la interfaz se llaman IDU (Interface Data Unit). Las IDU se forman con información de control local y la SDU (Service Data Unit) unidad de datos para el servicio. La SDU se fragmenta en PDUs (Protocol Data Unit), así por ultimo se procede al intercambio de mensajes con un formato común llamados unidades de datos de protocolo (PDU, Protocol Data Unit), que viajan por la red e implementan el propio protocolo.
Los protocolos controlan el intercambio de información entre unidades funcionales del mismo nivel tanto en la transmisión como en el control y recuperación de errores. Los protocolos de niveles diferentes son independientes y solo tienen que conocer la definición de servicios de su interfaz y no tiene nada que ver con los protocolos de los restantes niveles ni con los servicios de sus interfaces. Los protocolos de todos los niveles de un sistema forman una pila de protocolos.
Por lo tanto los principios del modelo son:
- La capa n ofrece sus servicios a la capa n+1 y esta solo usa los servicios de la capa n
- La comunicación entre capaz adyacentes de la misma pila se realiza mediante una interfaz.
- Cada capa se comunica con su capa equivalente (peer-to-peer) en el otro sistema utilizando un protocolo característico de esa capa (protocolo de capa n).
Estos principios son mostrados en la Fig.2.2.3

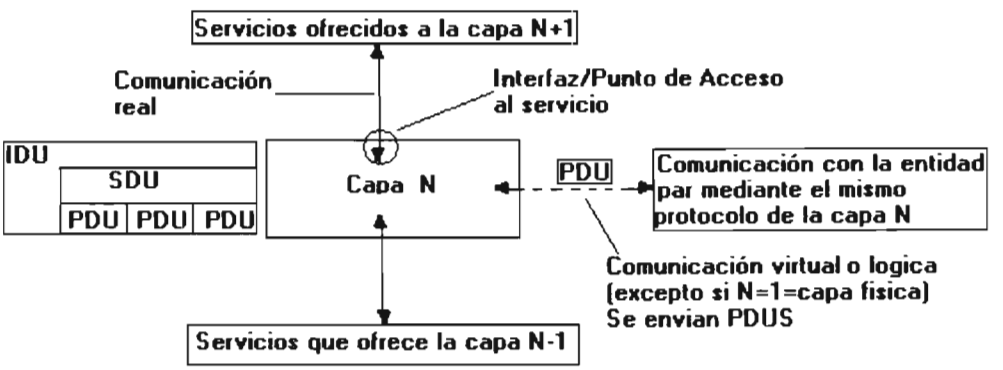


Fig. 2.2.3 Elementos de cada capa individual del modelo OSI

Transmisión de datos en el modelo OSI

La comunicación de datos entre dos nodos en el modelo OSI permite que los niveles pares de ambos nodos hablen entre ellos, para esto cada nodo debe tener el mismo protocolo de nivel.
El funcionamiento de la transmisión de datos de una red que sigue el Modelo de Referencia OSI se realiza de la siguiente forma, Fig.2.2.4:

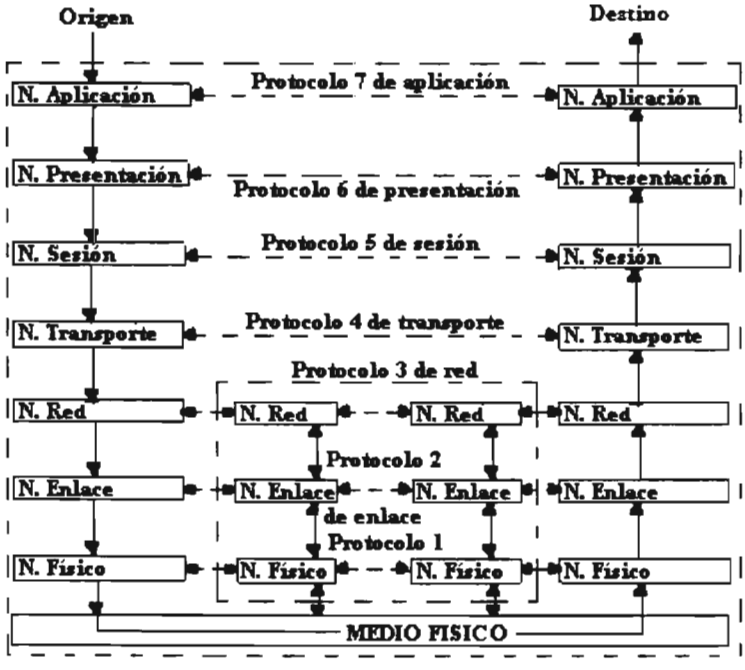


Fig. 2.2.4 Transmisión de datos en el modelo OSI.

Transmisión

- El nodo emisor pone a disposición del nivel de aplicación los datos a transmitir.
- El nivel de aplicación agrega a la información, proveniente del emisor, datos propios de la aplicación compuestos por una cabecera y cola de información, la información original mas los datos adicionales se pasan al siguiente nivel de presentación.
- El nivel de presentación hace el mismo proceso que el nivel de aplicación y pasa la información al nivel de sesión. Este mismo proceso se sigue hasta llegar al nivel físico donde se realiza la transmisión de la información a través del medio.

Recepción

- En el nodo receptor el mensaje que se recibe sufre el proceso inverso al del receptor a medida que asciende por los niveles del Modelo OSI, cada nivel procesa su cabecera y cola correspondientes y pasa la información sin esta cabecera al siguiente nivel superior.
- Finalmente los datos llegan al nodo receptor idénticamente como se enviaron desde el nodo emisor

Como se observa no se realiza una comunicación física directa entre los niveles del Modelo a excepción del nivel físico. La comunicación entre niveles puede ser directa pero de una manera lógica.
Los niveles del Modelo OSI se clasifican en dos grupos.

- Niveles de control también conocidos como capas superiores, los cuales están relacionados con las necesidades de comunicación entre usuarios finales.
- Niveles de transporte o capa inferiores, son los encargados de transferir los mensajes a través de la red.

2.3 Capas del Modelo OSI

Las 7 capas o niveles del Modelo OSI tienen funciones básicas y elementos propios de cada una, así como sus propios protocolos. Las tres capas de la parte superior del modelo (aplicación, presentación, sesión) son normalmente referidas como las capas superiores y sus funciones están muy relacionadas a facilitar la comunicación entre aplicaciones. Las siguientes dos capas (transporte y red) son las capas de en medio o capas de comunicaciones. Las capas mas bajas (enlace de datos y física) tratan con la parte física y eléctrica de los datos. Además de su nombre cada capa es a menudo referida por su número de capa.

2.3.1 Capa física

La capa 1 o capa física es el primer nivel o nivel mas bajo del Modelo OSI, se encarga de la definición de las especificaciones mecánicas, eléctricas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico.
La capa física maneja directamente el medio de transmisión, ocupándose de la transmisión de los bits a través de un medio físico, se asegura que cuando se transmita un bit con valor 1, se reciba exactamente igual en el otro extremo.
Sus funciones básicas son:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos. Definición y uso de cada pin de los conectores de la red.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento, y liberación del enlace físico).
- Manejar los voltajes y pulsos eléctricos utilizados para representar los bits de valor 0 ó 1.
- Transmitir el flujo de bits a través del medio.
- Definición del tiempo de duración en milisegundos de un bit.
- Garantizar la conexión (aunque no su confiabilidad) durante su establecimiento, y terminación al realizar transmisiones bidireccionales.
- Identificación de los circuitos de datos y su secuenciamiento.
- Administración del nivel físico.

Este nivel mas que manejar protocolos se constituye de estándares o normas para las interfaces utilizadas como: EIA RS-232 usada para la comunicación serial de computadoras, EIA-RS-449, CCITT X.21/X.21 bis, CCITT V35, define si conector es macho o hembra.. Hace la distinción entre quien es el equipo DTE (Data Terminal

Equipment) para referirse por ejemplo a un ordenador y DCE (Data Circuit-Terminating Equipment) para referirse a un modem.
Las normas de redes locales incluyen en sus especificaciones la capa física IEEE 802.3, Token Ring ISO 9314 o FFDI.

2.3.2 Capa de enlace

La capa 2 es responsable de mantener la integridad de los datos de una transmisión sobre un canal de comunicaciones. La capa de enlace proporciona a la capa de red un servicio de transito de datos confiable a través de un enlace físico, es decir hace al canal de transmisión confiable para la transmisión de los datos sobre un medio físico que normalmente no esta exento de ruido. En otras palabras este nivel se encarga de transformar el medio de transmisión ruidoso en una línea sin errores y por lo tanto confiable para el siguiente nivel de red. Este objetivo lo lleva a cabo dividiendo los datos en tramas de datos (constituidas por octetos), después realiza su transmisión en forma secuencial, y procesa las tramas de recibido que el receptor a su vez transmite. Esta capa crea y reconoce los limites de la trama insertando un patrón de bits especiales al inicio y termino de la trama, por lo que tiene que implementar algún mecanismo para recuperarse si esos bits se confunden con los datos debido a ráfagas de ruido, teniendo que retransmitir la trama, la cual a su vez se puede duplicar.
La capa de enlace de datos esta dividida en dos subcapas:

- La subcapa de control de enlace lógico (LLC). La subcapa LLC es la mas alta de las dos subcapas. Esta capa LLC administra comunicaciones entre dispositivos sobre una red (en un segmento de LAN). Es responsable de convertir los paquetes usados en la capa de red en tramas.
- La subcapa de control de acceso al medio (MAC). La subcapa MAC de la capa de enlace de datos es la interfaz entre la estación de trabajo y el medio de red. Es en la capa física donde cada dispositivo de red obtiene una dirección física o MAC. Esta es una dirección de 6 bytes (48 bits) que esta codificada en la tarjeta de red (o en la interfaz de red en un router). Los primeros 3 bytes son generalmente el identificador del fabricante, el cual es un valor hexadecimal asignado por el IEEE asignado al fabricante de tarjetas de red. Los últimos tres bytes son un único identificador de la tarjeta normalmente el numero serial de la tarjeta. Estas direcciones MAC también pueden ser definidas por software. Esta capa se comunica con la capa por debajo de ella que es la capa física. La subcapa MAC recibe las transmisiones electrónicas (los 1´s y 0´s) usadas para mandar datos a través del medio de transmisión física y los usa para construir tramas que pueden ser pasados a las capas superiores.

Entre las funciones de los protocolos del nivel de enlace de datos tenemos:

- Establecimiento y liberación de un enlace de datos en base a las siguientes fases:

- Iniciación. Se envían tramas de control entre las estaciones enlazadas para averiguar la disponibilidad de ambas para transmitir o recibir la información
- Identificación. Envío de tramas de identificación entre las estaciones para reconocerse mutuamente.
- Terminación. Cuando todos los datos han sido recibidos se produce la desconexión del enlace dejando libres los recursos.

- Estructura las tramas dividiendo los paquetes de datos en octetos y agregándoles una secuencia de bits al principio y al final de cada octeto, cada trama se compone de cientos de bytes.

- Control de la correcta transferencia de información resolviendo los problemas provocados por daño, perdida o duplicidad de tramas de acuse de recibido.
- Sincronización del envío de tramas, transfiriéndolas de una manera confiable libre de errores. Se establecen procesos para sincronizar el envió y recepción de los bloques múltiplos de 8 bits de información.

Para sincronizar la trama se define y se diferencia una trama del conjunto de información que se transmite para esto se anexa a la trama información de control que indica donde empieza y donde termina. Esto se puede hacer de tres formas:
- Usando caracteres especiales para indicar el principio y fin de la trama.
- Usando un carácter de principio de trama y un contador que indica el numero de caracteres de la misma.
- Usando un guión para indicar el principio y final de la trama.

La sincronización incluye el uso de protocolos que prohíben que el remitente envíe tramas sin autorización del receptor.

- Control, detección y recuperación de errores durante la transmisión en el nivel físico. La capa de enlace debe asegurar que cuando aparezca un error en la transmisión de una trama esta se detectara y posteriormente se recuperara, para detectar y controlar los errores se añaden bits de paridad, se usan códigos de redundancia cíclica y se envían acuses de recibo positivos y negativos y para evitar tramas repetidas se etiquetan con números de secuencia. Utiliza alguna de las técnicas siguientes:
  - Control directo de errores FEQ.
  - Petición automática de retransmisión ARQ.
  - Control de eco.
- Control de flujo para evitar que un transmisor muy rápido sature a un receptor muy lento. Esta función regula el ritmo de envío de tramas desde el transmisor al receptor si es que este ultimo tiene recursos para recibirlas. Para ello se pueden usar una de las siguientes técnicas:
  - Parada y espera. El emisor envía una trama y espera una señal de recibido (ACK) antes de enviar la siguiente.
  - Parada y arranque. El emisor envía tramas hasta que el receptor le indica que se detenga y con otra señal le indica que puede continuar transmitiendo.
  - Ventana deslizante. El receptor autoriza en cada instante el envío de un determinado número de tramas, el receptor renovara las autorizaciones según tenga disponibilidad para la recepción de las mismas.
- Control de la congestión de la red.
- Segmentación y bloqueo. Los mensajes largos se segmentan en tramas y los cortos se unen en bloques para adaptarlos a un formato acorde al enlace.
- Transparencia. Para eliminar la mala interpretación que se pueda dar si se transmite un conjunto de bits o caracteres similares a los de algún elemento de control del protocolo.
- Coordinación de la comunicación principalmente bidireccional mediante piggy backings para evitar conflictos de competencia por el uso del medio entre los acuses de recibido y la transmisión de datos mediante el retraso temporal del acuse de recibo de salida para que este pueda ser enganchado en la siguiente trama de salida. Se establecen procesos para evitar conflictos en el establecimiento de los enlaces por parte de las estaciones que lo solicitan. Existen dos métodos:

- Centralizado. La estación principal toma la responsabilidad del intercambio de información, enviándola al resto de las estaciones y sondeándolas cada cierto tiempo para recibir información de ellas, las cuales no pueden transmitir hasta que la principal lo autorice. Este método se usa en enlaces multipunto.
- Contienda. Se usa en enlaces punto a punto en el que cualquier estación solicita información en cualquier momento, implementando procedimientos para solucionar colisiones.

➢ Administración del propio nivel o enlace para que los datos accedan al medio.
➢ También se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos.

Las redes tipo broadcast usan funciones especiales de la capa de enlace para controlar el acceso al medio de transmisión ya que este es compartido por todos los nodos de la red. Esto hace un poco mas complejo a la capa de enlace lo que no sucede en las redes basadas en líneas punto a punto, por esta razón en las redes broadcast la capa de enlace se subdivide en dos subcapas, la inferior llamada subcapa MAC (Media Access Control) que se ocupa de resolver el problema de acceso al medio. Y la subcapa superior LLC (Logical Link Control) que cumple una función equivalente a la capa de enlace en las líneas punto a punto.
Como protocolos del nivel de enlace de datos tenemos:

- Protocolos orientados a carácter. Este tipo de protocolos fueron los primeros en usarse. BSC (Binary Synchronous Communications) de IBM, el SLC para empresas de transporte aéreo, SLIP, PPP.
- Protocolos orientados a bit. Son protocolos más modernos que los orientados a carácter:
  - HDLC (high-level Data link control) de ISO. Se considera que engloba a otros protocolos como SDLC, LAP, LAPB, LAPD, LAPX y LLC.
  - ADDCP (Advanced Data Communications Control Procedures) de ANSI.
  - LAPB (Link access procedure Balanced) del CCITT.
  - SDLC (Synchronous Data Link Control) de IBM.
  - BDLC (Burroughs Data Link Control) de Burroughs.
  - UDLC (Data Link Control Univac) de Univac.
  - LAP-B o X25 nivel 2 y LLC (Logical Link Control).
  - ISO 7776.
  - La capa de enlace X25 de ITU.
  - Protocolos de la subcapa MAC están los IEEE 802.3 para ethernet, IEEE 802.4, IEEE 802.5 Token Ring o el ISO 9314 para FDDI.
  - El protocolo de subcapa LLC de todas las redes locales tipo broadcast es el IEEE 802.2.

2.3.3 Capa de red

Debido a que la comunicación normalmente es en el ámbito de redes, el tráfico en estas es aleatorio y la distribución de usuarios es irregular, la capa de red es responsable de asegurar que la información se transmita correctamente a través de la red, por lo que esta capa se ocupa del control de la subred.
La responsabilidad primaria de esta capa es administrar las comunicaciones de extremo a extremo a través de la subred. Esto involucra asignar una dirección de red a ser usada para ruteo, mantener tablas de ruteo y calcular rutas optimas y controlar la congestión de la red. También es responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el

intercambio de datos entre el origen y el destino por lo que se tiene que conocer la topología de la red para poder determinar la ruta mas adecuada.
Proporciona a las entidades del nivel de transporte una transferencia de datos transparente proporcionándole conectividad y selección de la mejor ruta para la comunicación entre maquinas en lugares geográficamente distintos, con lo cual libera al nivel de transporte de conocer los mecanismos de la transmisión de los datos o tecnologías usadas para conectar los sistemas.
Sus funciones son la conexión y desconexión de redes, sincronización y control de flujo de las transferencias y la detección de errores en la transmisión recuperándolos en caso necesario. Si existe mas de una red implicada en la transmisión se encarga del encaminamiento de los paquetes entre las redes heterogéneas, es decir obtiene los paquetes procedentes de la fuente y los encamina por la red y subredes hasta alcanzar su destino, ya sea con rutas estáticas, o rutas definidas al empiezo de la conversación o rutas dinámicas determinadas por la carga de la red, también tiene que encargarse de resolver el problema de que alguna red no acepte el paquete en su totalidad, o que los protocolos sean diferentes, etc. Este nivel también introduce mecanismos para que en caso de alta demanda se pueda proteger la red de posibles sobrecargas.
Funciones del nivel de red:

- Estructurar los segmentos de la capa de transporte en unidades más complejas conocidos como paquetes a los que asigna las direcciones lógicas de los hosts que se están comunicando. Los tamaños de los paquetes son variables pudiendo llegar a ser muy elevados, sobre todo en protocolos recientes para poder aprovechar eficientemente la velocidad de los nuevos medios de transmisión (fibra óptica, ATM, etc). Por ejemplo en TCP/IP el tamaño máximo de paquete es de 64 kbytes pero en el nuevo estándar IPv6 el tamaño máximo puede llegar a ser de 4 Gbytes (4.294.967.296 bytes).
- Conocer la topología de la red y redireccionar los paquetes en el caso en que la maquina origen y la maquina destino estén en redes distintas.
- Asignar recursos para satisfacer la demanda.
- Distribución equitativa entre usuarios que compiten por los recursos.
- Distribuir la carga uniformemente entre los distintos elementos de la red.
- Control de la congestión para evitar cuellos de botella provocados por la presencia de muchos paquetes oponiéndose unos a otros.
- Proporcionar la contabilidad de la cantidad de paquetes, caracteres o bits mandados por cada usuario para obtener la información de tarificación.
- Encaminar la información a través de la red seleccionando la ruta a seguir por los paquetes transmitidos sobre la base de las direcciones del paquete, determinado los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers, switches).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Ensamblar los paquetes en el host destino.
- Permitir interconexión de redes heterogéneas para superar problemas de direccionamientos distintos entre redes, acondicionamiento del tamaño de los paquetes para que puedan ser procesados en cada red, manejo de los protocolos distintos en una red y en otra.
- En caso de ofrecer servicios de calidad QoS debe reservar los recursos necesarios para ofrecer el servicio prometido con garantías.

Los servicios que se proporcionan al nivel de transporte son:

- Enrutamiento: Para elegir el camino apropiado a seguir dentro de una subred.
- Control de congestión: Hace una selección de rutas para evitar sobrecargas o inactividad en las líneas de comunicación.
- Resolución de problemas de interconexión de redes.

Ejemplos de protocolos de la capa de red son:

- La conexión de red avanzada de par a par APPN (Advanced Peer-to-peer Networking) de IBM.
- Servicios de red orientado a la conexión CONS (Connection-Oriented Network Service), Servicio de red no orientado a la conexión CLNS (Connectionless Network Service),
- Protocolo de Internet IP (Internet Protocol) del grupo de protocolos de TCP/IP y UNIX.
- La parte de IPX del grupo de protocolos SPX/IPX de Novell.
- Interfaces de NetBEUI de Microsoft.
- Protocolo de distribución de datagramas DDP (Datagram Delivery Protocol) de Appletalk.
- CCITT/ITU-T Q931, Q933, Q2931.
- OSI CLNP (ConnectionLess Network Protocol).

2.3.4 Capa de transporte

La capa de transporte proporciona servicios a la capa de sesión mediante un mecanismo confiable para el intercambio de datos entre procesos entre dos entidades de sesión.

Los niveles superiores a partir del nivel de sesión se hacen independientes de los elementos de comunicación que constituyen la red por medio de este nivel, esto debido a que el nivel de transporte oculta a los niveles superiores los detalles específicos de la red a través de la cual se transmite la información de una forma segura, económica y con un transporte confiable de los datos. Para ello establece, mantiene y termina adecuadamente los circuitos virtuales proporcionando la confiabilidad del servicio con sistemas de detección y recuperación de errores de transporte.

Los circuitos virtuales son las conexiones que se establecen dentro de una red en las que no hay necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia una conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el trafico de datos posterior.

Este nivel pasa los datos del nivel de sesión al de red fragmentándolos en unidades mas pequeñas (segmentos) si es necesario y se asegura que todos lleguen correctamente a su destino en el cual los vuelve a reensamblar, aislando a la vez a la capa de sesión.

Para llevar a cabo el aseguramiento de la transmisión emplea funciones de direccionamiento, multiplexación, establecimiento de la conexión y desconexión y de transferencia y control de flujo de los datos. En modo normal crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si requiere de mucha transferencia de información puede crear múltiples conexiones de red, dividiendo los datos entre las conexiones para mejorar el caudal. O puede multiplexar varias conexiones de transporte sobre la misma conexión de red para reducir el costo de la red.

La conexión de transporte más popular es la de canal punto a punto sin error en la cual se entregan los mensajes en el mismo orden con que fueron enviados. Otros tipos de

conexiones de transporte son el servicio y transporte de mensajes aislados sin garantía acerca del orden de entrega y la distribución de mensajes a múltiples destinos. El tipo de servicio es determinado cuando la conexión es establecida.
En esta capa se ofrecen servicios de detección y corrección de errores para asegurar la integridad de los datos, así como los niveles de calidad de servicio, ya que la entidad de sesión podría especificar tasas de error aceptables, retardo máximo y prioridad.
Este nivel será más o menos complejo en función de la confiabilidad y tipo de servicio que proporcione el nivel de red. Cuanto más confiable sea el nivel de red más sencillo o menos funciones tendrá el protocolo de transporte.
Es la primer capa que se comunica directamente con su capa par de destino, establece comunicaciones del tipo extremo-a-extremo ya que un programa en la maquina origen conversa con otro en la maquina destino usando las cabeceras de los mensajes y los mensajes de control.
En el encabezado puede transportar la información que indica cuales mensajes pertenecen a cuales conexiones en el caso de hosts multiprogramados en los que se establecen múltiples conexiones por cada host.
Usa algún mecanismo para identificar o nombrar las conexiones para que un proceso en una maquina tenga una forma de describir con quien desea conversar.
La capa 4 divide a las 7 capas en capas extremo-a-extremo y capas encadenadas. Las capas 4-7 mantienen información de extremo a extremo, mientras las capas 1-3 mantienen comunicación con su vecino inmediato.
Las funciones de la capa de transporte son:

- Selección del servicio de red.
- Establecimiento y liberación de conexiones a través de la red.
- Aceptar los datos del nivel de sesión fragmentándolos en segmentos, estos segmentos se pasan a la capa de red para su envío.
- Determinación de la necesidad del multiplexado de varios flujos de mensajes en un solo canal.
- Optimización del tamaño de la unidad de datos.
- Mapeo de las direcciones de transporte en direcciones de red.
- Regulación del flujo de transacciones entre puntos finales para que un equipo más rápido no desborde al primero.
- Asegurar que se reciban todos los datos en el orden adecuado, realizando un control de extremo a extremo, mediante funciones de control y numeración de las unidades de información (segmentos).
- Reensamble de los mensajes en el host destino, a partir de los segmentos que lo forman.
- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Garantizar la transferencia de información a través de la red mediante la detección y recuperación de errores.
- Aplicar el proceso de queuing. La capa retiene temporalmente los segmentos para la transmisión.
- Aplicar el proceso de throtling back. La capa reduce la velocidad a la cual los datos son transmitidos a petición de una estación receptora ocupada o congestionada
- Aplicar el proceso windowing. Se establecen inicialmente parámetros de sesión entre las estaciones transmisora y receptora para optimizar las comunicaciones.

permitiendo al transmisor emitir algunos segmentos antes de recibir un reconocimiento (la estación receptora puede confirmar la recepción de dos o mas segmentos con un solo reconocimiento).

Ejemplos de protocolos del nivel de transporte son:

- APPN de IBM.
- Servicio de transporte orientado a la conexión COTS (connection-Oriented Transport Service) y Servicios de transporte no orientados a la conexión CLTs (Connectionless Transport Services de OSI).
- Del grupo de protocolos de TCP/IP de Internet y UNIX tenemos dos protocolos muy conocidos que son el TCP (Transmisión Control Protocol) y el UDP (User Datagram Protocol).
- Parte de SPX del grupo SPX/IPX de Novell.
- Interfaces NetBIOS y NetBEUI de Microsoft.
- Protocolo CCITT X.24 también llamado protocolo de Transporte OSI TP4 (transport Protocol 4).
- Protocolo de mantenimiento de la tabla de encaminamiento RMTP de AppleTalk

2.3.5 Capa de sesión

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host que se están comunicando por red organicen y sincronicen su dialogo y procedan al intercambio de datos. Para esto realiza el establecimiento de la conexión o sesión, usa la conexión para el intercambio de datos entre capas superiores e inferiores y desconecta la conexión o sesión entre maquinas diferentes de una red. Por sus tres fases para tratar una conexión se tiene un gran parecido con la capa de transporte. A través de esta sesión se lleva a cabo un transporte de datos ordinario. Se diferencia de la capa de transporte en los servicios que proporciona. De esta manera una sesión puede ser usada para permitir a un usuario iniciar sesión (log in) en un sistema remoto o para transferir un archivo entre dos maquinas.

Los servicios o funciones de este nivel son:

- Establecimiento de la conexión. Se realiza la conexión de dos entidades de presentación a petición del usuario.
- Administración de la sesión establecida entre los dos hosts.
- Intercambio de datos. Permite la transferencia de datos en uno o en ambos sentidos.
- Sincronización y mantenimiento de la sesión. Se realiza la sincronización y control entre las capas de presentación estableciendo las reglas o protocolos para el dialogo entre maquinas de manera que se produzca un intercambio ordenado de datos.
- Si una sesión falla por alguna causa ajena al usuario a la mitad de la transferencia de un archivo restaura la sesión a partir de un punto seguro y sin perdida de datos, si esto no es posible, termina la sesión de una manera ordenada, checando y recuperando todas sus funciones para evitar problemas transaccionales.
- Insertar puntos de control (checkpoints que son puntos de recuento en la transferencia de datos) en el flujo de bits para que al reestablecerse una sesión fallida la transferencia continúe donde se quedo para evitar la repetición de toda la operación.
- Administración del control de dialogo. Para esto la sesión permite que el trafico fluya en ambas direcciones al mismo tiempo o en una sola dirección caso en el cual

la sesión dará seguimiento de a quien le toca su turno y hará uso de fichas (token) para controlar y permitir la transmisión únicamente al extremo que posea el token. Esta es la base de algunos tipos de redes como Token Ring o FDDI.

- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Notificación de excepciones.
- Liberación de la conexión de sesión. Finalizado el intercambio de datos se procede a la desconexión.

Cada sesión se puede corresponder con una conexión de transporte o con varias, también varias sesiones pueden usar una misma conexión de transporte pero no a la vez.
Una vez liberada una conexión se establece otra sobre la misma conexión de transporte. Así después de que el nivel inferior transporta la información, abre una sesión en el otro extremo.

2.3.6 Capa de Presentación

La capa de presentación proporciona sus servicios a la capa de aplicación para garantizar que la información que envía la capa de aplicación de un sistema sea entendida y utilizada por la capa de aplicación de otro, establece el contexto sintáctico del dialogo. Este nivel se encarga de la transformación de los datos enviados por la red a los formatos requeridos por los protocolos de aplicación y viceversa. Aquí intervienen los aspectos sintácticos de la información, esto es, la forma o código en que se presentan los datos.
Aísla a las capas inferiores del formato de los datos de las aplicaciones encargándose de la semántica de los datos, ya que los datos que se quieren transmitir son números enteros, reales, caracteres, etc. Los datos en la red están en forma de bits como ASCII, EBCDIC, etc. Esto es, se precisa hacer una transformación de la representación utilizada en la red a la utilizada en la maquina y viceversa.
A través de este nivel los procesos de aplicación se hacen independientes de la representación de los datos e incluyen las posibles transformaciones de código.
El servicio que proporciona este nivel es la transformación de la sintaxis de los datos de la aplicación en la sintaxis de la presentación de los mismos.
Las funciones de este nivel son:

- Realizar la traducción de varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para esto convierte los datos desde el formato local al estándar de red y viceversa.
- Dar un formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario, así como aplicar procesos criptográficos.
- Definir la estructura de los datos a transmitir. Por ejemplo en el caso de un acceso a una base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC etc).
- Proporciona una forma de especificar y gestionar las estructuras de datos complejas que sean necesarias en las aplicaciones.
- Preserva el significado de la información, a diferencia de los niveles inferiores, que solo transmiten bits.

Las normas OSI para el nivel de presentación son:

- ISO 8822. Definición del servicio del nivel de presentación
- ISO 8823 Especificación del protocolo

- ISO 8824 Notación ASN.1
- ISO 8825 Reglas de codificación ASN.1

Ejemplos de protocolos de presentación son la compresión de texto o imágenes, el cifrado y el protocolo de terminal virtual. Por ejemplo el protocolo de terminal virtual realiza la conversión de las características de un terminal a las de un modelo virtual o genérico utilizado por los programas de aplicación.

2.3.7 Capa de aplicación

Esta capa es la interfaz donde al usuario se le muestra la información recibida y donde residen las aplicaciones. Proporciona diferentes servicios a las aplicaciones y al usuario final, definiendo los protocolos usados por las aplicaciones individuales.
La capa de aplicación es la capa que se encuentra en la parte mas alta de la torre de niveles del modelo OSI, su misión es controlar y coordinar las funciones a realizar por los programas de usuarios de manera que le permita el acceso al ambiente OSI. Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación, las cuales están controladas por protocolos de aplicación utilizando servicios de la capa de presentación.
Esta capa ya no proporciona servicios a ninguna otra capa OSI solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.). Asimismo establece la disponibilidad de los elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre si y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.
Para entender un poco mas la función de esta capa considere el caso del uso de un editor de pantalla completa en una red con diferentes tipos de terminales, cada terminal tiene su diseño de pantalla para las secuencias de escape, inserción y borrado de texto, etc. Para dar una solución a este problema se puede definir una terminal virtual, para lo cual los editores y otros programas puedan ser escritos para trabajar con ella. Así para manejar cada tipo de terminal una pieza de software se tiene que escribir para asignar las funciones de la terminal virtual en la terminal real. De esta manera cuando el editor mueva el cursor de la terminal virtual a la esquina superior izquierda de la pantalla, el software debe emitir la secuencia de comando apropiada a la terminal real para que lleve su cursor allí también. Todo el software de la terminal virtual esta en la capa de aplicación.
Puede haber tres tipos de procesos de aplicación:

- Procesos propios del sistema. Son los procesos que ejecutan funciones para controlar y supervisar las operaciones de los sistemas conectados a la red de comunicación.
- Procesos de gestión de aplicaciones. Procesos que controlan y supervisan las operaciones de los procesos de aplicación.
- Procesos de aplicación de usuario. Son los que procesan la información real para los usuarios.

Ejemplos de programas que usan servicios de la capa de aplicación más comunes son:

- Administración y transferencia de archivos con los cuales se manejan incompatibilidades en la forma de nombrar los archivos en sistema diferentes, las formas de representar las líneas de texto.
- Correo electrónico.
- Administración de red.

- Navegación en Internet.
- Trabajo a distancia mediante terminales virtuales.
- Búsqueda de directorios.

Algunos estándares que funcionan en esta capa son:

- X.400.
- SMTP (Simple Mail Transfer Protocol).
- SNMP (Simple Network Management Protocol).
- FTP (File Transfer Protocol).
- TFTP (Trivial File Transfer Protocol).
- Telnet.

La Fig. 2.3.1 nos muestra las siete capas del modelo y sus funciones

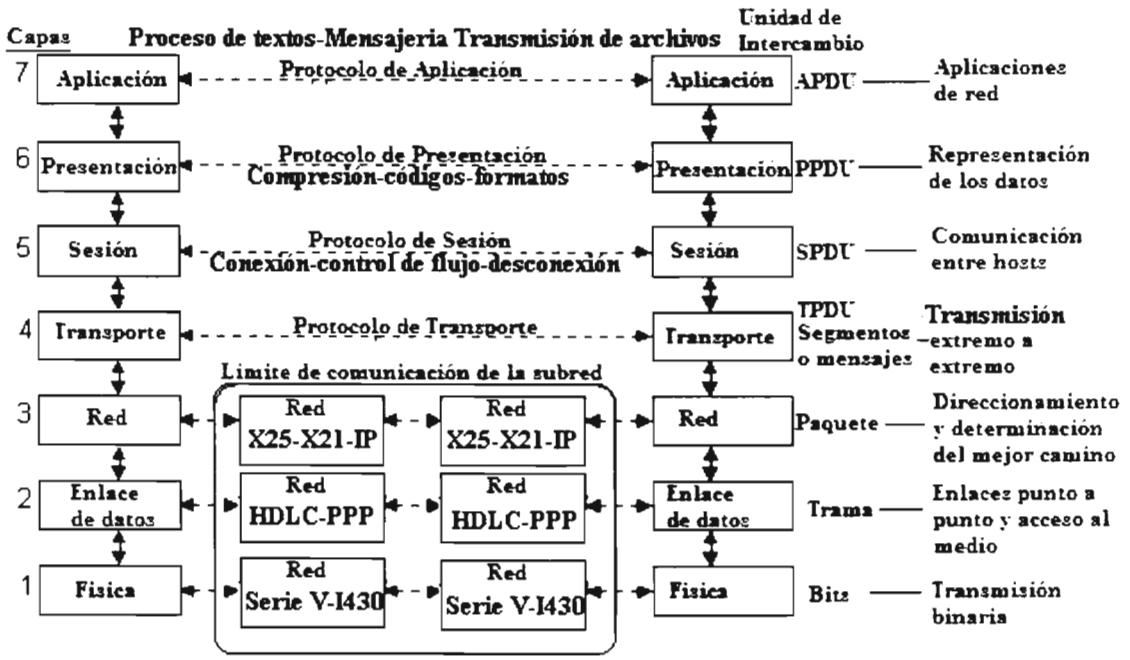


Fig. 2.3.1 Las siete capas del modelo OSI y sus funciones.

Encapsulamiento

El procesamiento de la información al pasar por una red basada en el modelo OSI sufre una modificación en cada una de las capas del modelo, esta modificación no es de contenido, se realiza para adaptar los datos de manera que puedan ser tratados por los diferentes niveles. El proceso que hace esto es la encapsulación.

Cuando las aplicaciones envían los datos desde el origen estos viajan a través de las diferentes capas. Las tres capas superiores (aplicación, presentación y sesión) preparan los datos con un formato común para su transmisión. A partir de aquí se aplican diferentes encapsulamientos. Este proceso de encapsulamiento se realiza en cinco pasos:

1. Creación de los datos (capa de presentación). Cuando por ejemplo se envía un mensaje de correo electrónico los caracteres alfanuméricos del mensaje se convierten en datos que pueden recorrer la red.

2. Los datos se empaquetan para ser transportados de extremo a extremo (capa de transporte). Para esto se dividen los datos en unidades manejables, segmentos, y se les asigna números de secuencias para que el receptor los pueda volver a unir. Se empaquetan para ser transportados por la capa de red.
3. Se agrega la dirección de red al encabezado (capa de red). La capa de red encapsula al segmento creando un paquete o datagrama y le agrega las direcciones lógicas de red de la maquina origen y de la maquina destino con las cuales se enrutan los paquetes a través de la red.
4. Se agrega la dirección local al encabezado de enlace de datos (capa de enlace de datos). En esta capa se encapsula el paquete para formar una trama, se le agrega a la trama las direcciones MAC (numero de la tarjeta de red, único para cada tarjeta) origen y destino, después transmite los bits de la trama a través de los medios de la capa física.
5. Se transmite el tren de bits creado (capa física)

Este proceso de encapsulamiento se muestra en la Fig. 2.3.2

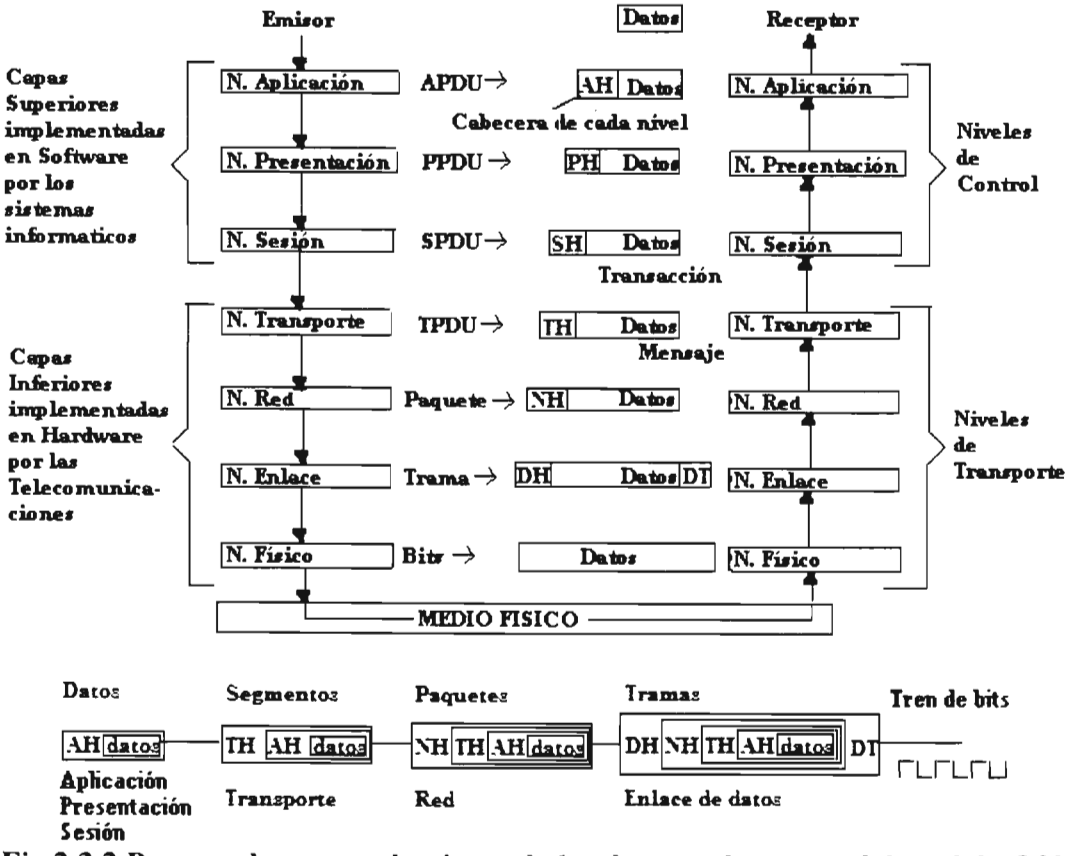


Fig.2.3.2 Proceso de encapsulamiento de los datos en las capas del modelo OSI

2.4 Servicios del modelo OSI

Cada una de las capas del modelo OSI recibe servicios de la capa inferior y suministra servicios a la capa superior para comunicarse con su par en el otro extremo. En función de cómo se establezca esa comunicación pueden distinguirse dos tipos de servicios:

- Servicios orientados a conexión
- Servicios no orientados a conexión.

2.4.1 Servicios orientados a conexión

Los servicios orientados a conexión CONS (Connection Oriented Network Service) son servicios confiables por que la transmisión de datos esta controlada en cada momento pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos.
La característica de estos servicios es la confiabilidad para realizar la comunicación de datos mediante el siguiente proceso:

1. Primero se establece una conexión por el canal de comunicaciones.
2. Una vez establecida la conexión se realiza la transmisión de los datos.
3. Por ultimo cuando ya se han transmitido todos los datos se termina la conexión.

La conexión que se establece se denomina circuito virtual VC (Virtual Circuit). Una vez establecido el VC, el camino físico que van a seguir los datos esta determinado; los paquetes deben transmitirse por el VC desde el origen al destino y llegar en el mismo orden en que han salido, este VC funciona como un tubo a través del cual se envía por un extremo la información continuamente, mientras que en el otro extremo los mensajes llegan en el orden en que fueron enviados y sin errores, esta forma de llevar la información hace a estos servicios una forma confiable de comunicación de datos, en forma parecida al sistema telefonico.
Ya que el VC establece de forma clara el destino, los paquetes no necesitan contener su dirección.
Generalmente se distinguen dos tipos de circuitos virtuales: los circuitos virtuales conmutados SVCs (Switched Virtual Circuit) y los circuitos virtuales permanentes PVCs (Permanente Virtual Circuit).
Los SVCs se establecen y terminan a petición del usuario, normalmente cuando hay paquetes que se quieren transmitir, es decir se establecen cuando se van a usar y se terminan cuando ya no se van a usar.
Los PVCs están establecidos todo el tiempo que la red esta operando, quedan permanentemente establecidos se usen o no.
Otra característica de los servicios confiables es que el receptor envía acuses de recibo o notificaciones para informarle al emisor que recibió los datos transmitidos. De esta manera el emisor esta seguro que la información llega a su destino.
Este proceso de notificación introduce un exceso de tráfico y retardos necesarios para dar confiabilidad a la transmisión,
Los servicios confiables son muy útiles por ejemplo en la transferencia de archivos en los cuales nos interesa que la información sea recibida correctamente en el otro extremo.

2.4.2 Servicios no orientados a conexión

Los servicios no orientados a conexión CLNS (ConnectionLess Network Service) son también conocidos como servicios sin conexión o no confiables ya que no tienen un control de los datos transmitidos y por lo tanto no pueden garantizar que se hayan recibido todos los datos.
En el CLNS la comunicación se establece de manera informal. Cuando una entidad tiene información que transmitir solamente la envía en forma de paquetes, confiando

que estos llegaran a su destino en algún momento dado. No se establece préviamente un VC ni otro tipo de canal de comunicación extremo a extremo.
Aquí la información no se envía de forma continua y el camino que toma cada mensaje es independiente. Cada uno de los paquetes que forma al mensaje debe incluir cada uno la dirección completa de su destino.
Por ejemplo al enviar dos mensajes lo más normal es que el mensaje que se envió primero llegue antes que el segundo, es decir que lleguen en el mismo orden de salida, esto no esta garantizado como en el CONS debido al almacenamiento de nodos intermedios y a la diversidad de caminos físicos posibles, el primero puede sufrir un retraso y llegar después que el segundo. Por esto el servicio no es confiable pues la capa de red no garantiza el orden de los paquetes ni controla su flujo por lo que los paquetes deben llevar sus direcciones completas de destino. Una analogía a este servicio es el correo convencional.
A los paquetes enviados en un servicio no orientado a conexión se les denomina datagramas ya que cada paquete viaja hacia su destino de forma completamente independiente de los demás como si fuera un telegrama, en los telegramas tampoco hay una confirmación de que la información llego sin problemas.

En cualquiera de los dos tipos de servicio CONS o CLNS puede haber perdida de información; también puede ocurrir que en el tiempo de envió del paquete haya retraso también llamado retardo o latencia (delay y latency) o que ese mismo tiempo sea demasiado grande o fluctué (la fluctuación se conoce como jitter) dentro de un amplio rango debido a la carga o congestión en la red.
En algunos casos se requiere una entrega confiable, o sea que se garantice la entrega de los paquetes o un retardo y/o jitter garantizados no superiores a un determinado valor. Así por ejemplo para transferir un fichero normalmente se divide en múltiples paquetes, se necesita un servicio confiable en la entrega pero se puede tolerar un retardo o jitter más o menos grande; por el contrario la voz o el video toleran un pequeño porcentaje de pérdidas pero requieren un retardo y un jitter reducidos y constantes.
Cuando al establecer una comunicación se solicita un nivel mínimo para alguno de estos parámetros se dice que se requiere una calidad de servicio QoS (Quality of Service). La calidad de servicio estipula unos mínimos que la red ha de satisfacer para efectuar la conexión. No todos los protocolos o redes ofrecen la posibilidad de negociar calidades de servicio; en estos casos el protocolo simplemente aprovecha los medios disponibles lo mejor que puede, intentando evitar las congestiones y situaciones criticas en lo posible y repartir los recursos entre los usuarios de manera mas o menos equilibrada, esta estrategia se denomina del mejor esfuerzo. Ejemplos de redes con calidad de servicios tenemos una red ATM, ejemplo de redes de mejor esfuerzo son TCP/IP y Ethernet.

Primitivas de servicio
En el modelo OSI cada capa ofrece sus servicios a la siguiente. El servicio es el conjunto de operaciones u ordenes que la capa superior puede mandar a la capa inferior. Este conjunto de operaciones son las primitivas.
Las primitivas se pueden analizar con el establecimiento y terminación de una conexión entre la capa n de dos sistemas A y B. Fig. 2.4.1

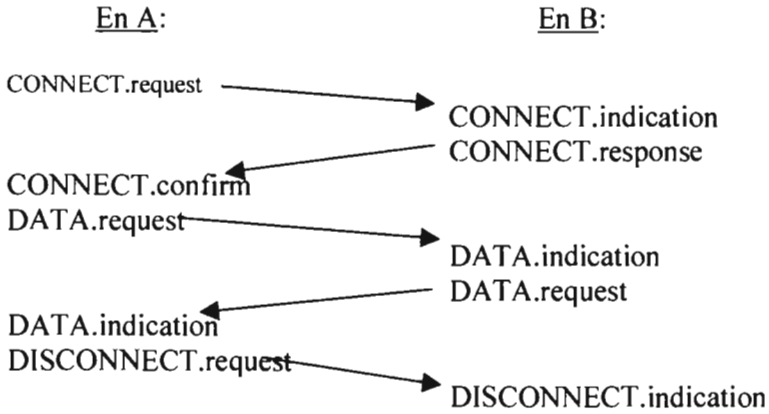


Fig. 2.4.1 Primitivas de servicio

La entidad A.n (esto se lee como la capa n del sistema A) inicia una conexión emitiendo una primitiva CONNECT.request, con esta primitiva se transfiere una IDU (Unidad de datos de Interfaz) a través del SAP(Punto de Acceso al Servicio) a la capa inferior (entidad A.n-1), esta extrae la información de control, y crea la SDU (Unidad de datos de servicio) que convierte en una o varias PDUs (Unidades de datos de protocolo). Estas PDUs se trasfieren al sistemas B, y llegan a la entidad B.n-1, esta entidad regenera la SDU, la información de control y con ello la IDU, la cual transmite a la entidad B.n a través del SAP mediante la primitiva CONNECT.indication que le indica a B.n que alguna entidad desea establecer conexión con ella. Entonces B.n emite la primitiva CONNECT.response para indicar si acepta o rechaza la conexión. La respuesta se manda en un paquete de B.n-1 a A.n-1, esta última informa a A.n de la situación mediante la primitiva CONNECT.confirm.
Este es un servicio confirmado por que se verifico que la conexión se establece, para esto se envía un paquete en cada sentido.
Se puede establecer una conexión no confirmada para la cual solo se emiten el request y el indication. Una vez establecida la conexión se transfieren los datos y se termina la conexión.

2.5 Redes de comunicación de datos

El uso de las redes de comunicación de datos ha tenido un gran éxito gracias a las ventajas que proporcionan en la transmisión de datos, compartición de recursos y eficiencia de las actividades laborales. Es tal el éxito de las redes que podemos encontrarlas en el trabajo, escuelas, hogar, etc. La prueba mas clara del éxito de las redes de datos es el uso, crecimiento y desarrollo de la red de redes Internet.
El gran éxito y utilidad de las redes se encuentra en el objetivo para el que fueron creadas, el objetivo de una red de computadoras es compartir recursos y hacer que todos los programas y los equipos estén disponibles para cualquiera en la red, donde el recurso más importante es la información.

2.5.1 ¿Qué es una red?

Una red es un sistema de transmisión de datos que permite el intercambio y compartición de información de forma rápida y eficiente entre un conjunto de dispositivos tales como computadoras (personales, mini computadoras, mainframes), terminales interactivas, elementos de memoria, impresoras, dispositivos de comunicaciones, asistentes personales (PDA), televisores Web, aparatos electrodomésticos conectados a Internet, etc., conectados entre sí que permiten a los usuarios hacer transferencias de datos y compartir recursos de hardware y software (los recursos pueden ser archivos, impresoras, aplicaciones especificas de red, prestaciones cliente/servidor, unidades de CD-ROM, unidades ZIP, discos duros, faxes, módems, acceso a Internet) e información (informes, hojas de calculo, facturas, correos electrónicos, videos, imágenes, musica, ilustraciones, fotografías, videos, audio, bases de datos, paginas web, etc.) a la vez que permite realizar comunicaciones electrónicas. La transmisión de los datos se puede realizar a través de algún medio de transmisión o una combinación de diferentes medios (cables, fibra óptica, tecnología inalámbrica, enlaces vía satélite, etc.).

Entre otras cosas las causas de la creación y desarrollo de las redes de transmisión de datos fueron el aumento de la popularidad y uso de las computadoras personales como herramientas de trabajo en las actividades diarias del hombre se volvió indispensable para el desarrollo eficiente de dichas actividades y funciones. A la par con esa importancia las computadoras se fueron haciendo cada vez más potentes pudiendo procesar y manipular rápidamente grandes cantidades de datos. Pero todo el trabajo y procesamiento de las computadoras se realizaba en forma aislada, así, los usuarios tenían que imprimir sus documentos o almacenarlos en discos para poderlos compartir con otros usuarios, las modificaciones que hiciera uno y otro usuario a la información no podía ser combinada inmediatamente con la que ya poseía la otra parte. Situaciones como estas crearon la necesidad de conectar las computadoras en red para realizar actividades como intercambio de mensajes, compartir aplicaciones, datos y dispositivos como impresoras, unidades de almacenamiento, líneas de telecomunicación, etc.
Las redes fueron creadas para realizar la interconexión y compartición de forma rápida y eficiente, lo que hace atractivo al concepto de una red de datos es la combinación de los

términos compartir-rapidez-eficiencia, ya que si la compartición de datos por medio de una red es muy lenta no representa ventaja alguna en cuanto al sistema de compartir la información en disco.
En su nivel más elemental, una red consiste en dos equipos conectados entre sí con un cable que les permite compartir datos. De esta manera si un equipo esta conectado a otros puede compartir datos con ellos y enviar documentos a otras impresoras. Esta interconexión de equipos y otros dispositivos se llama una red y el concepto de conectar equipos que comparten recursos es un sistema de red.
El uso de una red de computadoras se justifica por que las redes aumentan la eficiencia y reducen los costos en las empresas mediante la realización de tres funciones principales:

- Comparticion de información o datos.
- Comparticion de hardware y software
- Centralización de la administración y el soporte.

Compartición de información (archivos o datos)
La capacidad de compartir cualquier tipo de información ya sea archivos, datos, imágenes, documentos, música, correo electrónico, video, etc. de forma rápida y económica ha sido el principal uso de la tecnología de las redes locales. Así un usuario en su estación de trabajo puede usar ficheros de otros usuarios sin gastar en el uso de un disquete para almacenar la información y sin perder tiempo trasladándose al lugar de otro usuario. La ventaja fundamental es disponer de directorios en la red a los que tienen acceso grupos de usuarios y en los que se puede guardar información que comparten dichos grupos. Así por ejemplo las empresas pueden invertir en las redes para aprovechar las facilidades de comunicación de los programas de correo electrónico. Al hacer que la información se pueda compartir, por ejemplo se puede reducir la comunicación por escrito incrementando la eficiencia, a la vez que permite que cualquier tipo de dato este disponible simultáneamente para cualquier usuario que lo necesite.

Compartición de hardware
Antes de conectar los equipos por medio de redes los usuarios necesitaban sus propias impresoras, trazadores y otros periféricos. Con las redes locales los usuarios pueden acceder a impresoras de calidad y alto precio sin necesidad de instalar una para cada usuario y sin que estos tengan que llevar su información en disquete para imprimir en otra maquina, para lo cual se instalan una o dos impresoras que los usuarios pueden compartir a través de la red.
Cuando se comparte una impresora de la red, se pude conectar una impresora a una estación de trabajo que actúa como servidor de impresión, esta estación de trabajo puede ser el equipo de un usuario, entonces todos los demás usuarios usaran la impresora desde la estación del usuario que la tiene instalada directamente.
También se puede tener una impresora que ya disponga directamente de una tarjeta de red con lo que la impresora se conectara directamente a la red sin necesidad de depender de una computadora y sin tener que situarla cerca de alguna maquina.
De la misma manera si una maquina tiene configurado un modem para usarlo como fax puede permitir que el resto de los usuarios de la red lo utilicen para enviar sus propios documentos. En general de esta misma forma todas las computadoras en red pueden compartir el hardware que poseen o que tienen conectado.

Compartición de aplicaciones de red
Las redes pueden usarse para compartir y estandarizar aplicaciones. Hay un gran número de aplicaciones que aprovechan las redes locales para que el trabajo sea más eficiente. Aplicaciones como el correo electrónico permite el intercambio de mensajes entre los usuarios, mensajes que pueden consistir de texto, sonido, imágenes, además que puede llevar asociado cualquier tipo de archivo. De esta manera se pueden sustituir ciertas reuniones o realizar el análisis mas detallado del material que los otros usuarios nos permitan conocer. Asimismo se pueden compartir aplicaciones de procesadores de texto, hojas de cálculo, bases de datos, etc. Todo esto asegura que los usuarios utilizan las mismas aplicaciones y las mismas versiones de esas aplicaciones. Esto permite hacer la compartición más fácil y eficiente a la vez que es mejor que los usuarios aprendan a usar bien una sola aplicación a tener que manejar diferentes versiones o aplicaciones.

Aplicaciones cliente/servidor
Las redes locales ayudan a las aplicaciones que manejan grandes volúmenes de información. Los programas pueden dividir su trabajo en dos partes, una parte cliente que se realiza en la estación del usuario y otra parte servidor que se realiza en un servidor con dos fines:

- Aliviar la carga de trabajo de la estación cliente.
- Reducir él tráfico de la red.

Por ejemplo para consultar en un servidor una base de datos en un esquema que no es cliente/servidor al hacer la petición desde otra estación el servidor enviara todos los registros de la base de datos elevando el tráfico de la red. Con aplicaciones cliente/servidor se le envía la consulta al servidor y este realiza la búsqueda de la información que se desea y solamente devuelve a la estación que lo solicito los resultados de la búsqueda, de esta manera disminuye el trafico de la red y la estación cliente obtiene el resultado para poder realizar su trabajo.

Acceso a Internet
Para poder acceder a Internet se puede configurar una computadora-servidor con una línea permanente de alta velocidad a Internet, cuando un usuario por medio de la red activa la conexión en el servidor, esta quedara disponible para todos los demás usuarios, de esta manera no se necesitan módems personales por usuario para conectarse a Internet.

Centralización de la administración y el soporte
Aunado a todo lo anterior las redes de computadoras facilitan las tareas de soporte y administración de las mismas, ya que para el personal de soporte técnico es más eficiente dar soporte a una sola versión de sistema operativo, aplicación o hardware que tener que soportar muchos sistemas y configuraciones individuales y diferentes.

Las redes de computadoras están regidas por protocolos que engloban a un conjunto de normas. Estas normas especifican que tipo de cables se utilizaran, la topología que tendrá la red, la velocidad a la que trabajaran las comunicaciones y la forma en que se accederá al canal de transmisión.

2.5.2 Clasificación de las redes de datos

Las redes de datos se pueden clasificar sobre la base de tres características, su tecnología de transmisión, su tamaño o escala y su topología:

- Clasificación por su tecnología de transmisión:
  - Redes punto a punto o conmutadas.
  - Redes de difusión.
- Clasificación por su tamaño o escala:
  - LAN
  - MAN
  - WAN
- Clasificación por su topología. Esta clasificación es más aplicable a las redes LAN

En este tipo de clasificación tenemos primeramente una clasificación por la forma de distribución de los componentes:

- Topología en BUS.
- Topología en Anillo.
- Topología en Estrella.

Asimismo dentro de la clasificación por topología se puede hacer una distinción por el tipo de tecnología:

- Ethernet
- Token Ring
- FDDI

2.5.2.1 Clasificación por tipo de transmisión

Dependiendo de la arquitectura y la forma o tecnología de transferir la información las redes de comunicación de datos se clasifican en:

- Redes punto a punto o conmutadas.
- Redes de difusión.

- **Redes punto a punto o conmutadas.**

En las redes punto a punto un conjunto de nodos se interconecta entre sí a través de medio de transmisión formando una topología en forma de malla, es decir, consisten en muchas conexiones entre pares individuales de maquinas.

La información se transmite encaminándola del nodo origen al nodo destino mediante la conmutación entre nodos intermedios.

Un nodo realiza la conmutación ya sea física o lógica de un camino de entrada al nodo a un camino de salida al nodo para realizar la transmisión de la información de su entrada a su salida. A su vez las redes conmutadas se subdividen en:

- Conmutación de paquetes.
- Conmutación de circuitos.

➢ **Conmutación de paquetes**

En las redes de conmutación de paquetes los nodos dividen la información que quieren enviar en paquetes. Cada paquete se envía por el medio de transmisión con una información de cabecera. En cada nodo intermedio por el que pasa el paquete se procesa para determinar hacia donde se dirige.

Para llegar del origen al destino un paquete tendrá que pasar por maquinas intermedias y tendrá que viajar por varias posibles rutas de longitud variable, por lo que en este tipo de redes se tienen que implementar algoritmos de ruteo.

➢ **Conmutación de circuitos.**

En este tipo de redes dos nodos se conectan usando en forma exclusiva para ellos el circuito físico que los conecta durante la transmisión. En cada nodo intermedio de la red se cierra un circuito entre la entrada y la salida de la red.

Un ejemplo de este tipo de redes son las redes telefónicas públicas.

Como regla general las grandes redes suelen ser punto a punto.

- **Redes de difusión**

En las redes de difusión no existen nodos de conmutación, tienen un solo canal de comunicación compartido por todas las maquinas de la red. Los mensajes o paquetes que componen la información transmitida por un nodo son escuchados por todas las demás. Debido a que el mensaje llega a todas las maquinas debe haber alguna forma de indicar para quien esta dirigido el mensaje, por eso dentro del mensaje se incluye un campo de dirección que especifica a quien se dirige y por lo tanto quien debe procesarlo. La difusión o broadcast que se realiza puede ser de dos tipos:

- Multicast (Multidifusión). Es una forma de broadcast en el cual el paquete es liberado sobre la base de un conjunto predefinido de posibles direcciones de destino. Esto es, de todas las computadoras que componen la red y que reciben el mensaje solo algunas de ellas procesaran el mensaje ya que va dirigido solamente a algunas, no a todas.
- Unicast (Unidifusión). En este caso una trama es enviada de una computadora a otra. El unicast contiene una dirección MAC específica de los dispositivos origen y destino. Es decir, el mensaje llega a todas las computadoras pero solo una lo procesara por que es a quien va dirigido.

Como una regla general las redes pequeñas tienden a usar la difusión como es el caso de las redes Lan. Otros ejemplos de estas redes de difusión es la comunicación por radio o por satélite.

2.5.2.2 Clasificación por tamaño

Esta clasificación solía hacerse sobre la base de las distancias que cubría cada tipo de red, en la actualidad se puede definir esta clasificación de tipos de redes sobre la base de su ubicación geográfica, así tenemos una clasificación básica que consiste de 3 tipos (aunque suelen manejarse más):

- Red de área local LAN (Local Area Network)
- Red de área metropolitana MAN (Metropolitan Area Network)
- Red de área extensa WAN (Wide Area Network)

- **Red de área local LAN**

Una red de área local es un sistema de comunicaciones de datos a alta velocidad y bajos niveles de error que cubre un área geográfica relativamente pequeña (edificio u oficina, universidad) o que esta restringida geográficamente (hasta unos pocos de miles de metros, en este tipo de red no habrá por lo general dos estaciones de trabajo que disten entre sí más de un kilómetro) y proporciona la interconexión a una variedad de dispositivos permitiéndoles compartir los recursos de la red como archivos, periféricos, impresoras así como el intercambio información. Las redes de área local no utilizan medios de telecomunicación externos.

Una configuración típica en una red de área local es tener una computadora que funciona como servidor de ficheros por ejemplo, en la que se almacena todo el software de control de la red, así como el software que se comparte con los demás ordenadores de la red, estos son menos potentes y suelen tener software personalizado por cada usuario.

La mayoría de las redes Lan están conectadas por medio de cables y tarjetas de red en cada equipo.

Las redes LAN son las mas conocidas de la clasificación por tamaño ya que son las que interconectan computadoras a alta velocidad y bajo costo.

Con las computadoras o estaciones personales conectadas por medio de una LAN se generan grandes ventajas como la reducción en el costo de la tecnología, interfaces graficas de usuario, reducción del ciclo de desarrollo de aplicaciones, las aplicaciones se diseñan en forma modular, delegación y gestión de las aplicaciones por el usuario.

De la anterior definición tenemos cuatro elementos importantes en la definición de una red LAN:

- El conjunto de elementos que forman el sistema de comunicaciones cuyo objetivo es el intercambio de información entre dispositivos.
- Los dispositivos que en forma genéricamente abarcan todo, son cualquier nodo de la red, desde un gran procesador hasta una computadora personal, pasando por estaciones de trabajo, impresoras, etc.
- El ámbito geográfico de una red local se reduce a un edificio o algunos edificios.
- La propiedad de los medios de comunicación es privada.

Las LANs conectan y comparten información, estaciones de trabajo, periféricos terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Las Lan están estandarizadas cuyas normas especifican el cableado y señalización en las capas física y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

- **Red de área metropolitana MAN**

Las redes MAN cubren áreas metropolitanas de extensiones mayores que las LAN como puede ser una ciudad o un distrito. Estas redes se forman interconectando redes LAN, para distribuir la información a los diferentes puntos del distrito. Las bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

- **Redes de área amplia WAN**

Las redes WAN salen del área de la MAN, o sea salen de una ciudad y cubren un estado o grandes regiones como un país, un continente o incluso el mundo. Cables transoceánicos o satélites se utilizan para enlazar puntos que distan grandes distancias entre sí. El uso de estas redes permite comunicar lugares muy distantes sin pagar cantidades enormes de dinero como sucede en la comunicación por teléfono. Se tiene que hacer uso de equipo y técnicas que permitan que redes de diferentes características se puedan comunicar sin problemas. El mejor ejemplo de una red WAN es Internet.

En esta clasificación de red WAN que abarca todo el mundo tal vez haya cierta discrepancia ya que existe un gran número de literatura de redes que limitan el alcance de una red WAN a todo un país y para abarcar áreas mayores se tienen otras clasificaciones. Mencionaremos estas otras clasificaciones para tenerlas presentes, no sin antes recordar que se menciono anteriormente que se tenían tres clasificaciones básicas, donde en la red WAN se incluye el área desde un país hasta todo el mundo.

- Red de un Campus o CAN (Campus Area Network)

Es una red que abarca un conjunto de edificios ubicados en la misma área

- Red de Área Global GAN (Global Area Network)

Es una red que abarca diferentes países por ejemplo Internet.

- Red PAN (Personal Area Network)

Es una red casera personal con por lo menos dos computadoras y un equipo de conectividad

2.5.2.3 Clasificación por topología

La topología de una red se determina por la forma como se utiliza el medio de transmisión para interconectar los diferentes dispositivos así como la logística de distribución de los elementos de la red, esta distribución forma el patrón de interconexión entre nodos y servidor. En el contexto de las redes LAN la topología tiene dos acepciones que son:

- La topología lógica que se refiere a como funciona la LAN, describiendo como se transmiten los mensajes desde un dispositivo a otro y la forma en que es controlado el flujo de los datos.
- La topología física se refiere a la apariencia física que se basa en la distribución del cableado de la red que interconecta las diferentes computadoras, es decir es el mapa de distribución del cable que forma la intranet.

Existen tres topologías físicas puras:

- Topología en BUS o bus lineal.
- Topología en anillo.
- Topología en estrella (STAR).

De la mezcla de topologías físicas se originan las topologías lógicas que hacen el funcionamiento de una topología física más eficiente:

- Topología de Árbol (Tree)
- Topología anillo-estrella o tecnología Token Ring FDDI, CDDI

- **Topología en BUS**

En la topología en bus lineal todos los elementos o nodos de la red están conectados directamente a través de interfaces físicas llamadas tomas de conexión a un único medio de transmisión compuesto por un cable central que es el bus, también llamado backbone o segmento por el cual se envían o reciben las señales de información entre los equipos, Fig. 2.5.2.3.1.

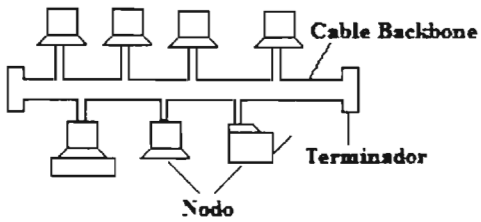


Fig. 2.5.2.3.1 Topología de Bus

El bus debe tener conectados en cada extremo una resistencia llamada terminador el cual permite cerrar el bus además que evita que las señales reboten y regresen al bus, y es un indicador de que ya no hay mas computadoras conectadas en el extremo.

Se permite la transmisión full duplex ya que cada estación puede recibir o transmitir, y la señal de transmisión de cada estación se propaga a ambos lados del emisor hacia todas las estaciones conectadas al bus, hasta llegar a los puntos de terminación donde la señal es absorbida, de aquí que el bus también reciba el nombre de canal de difusión.

Las redes de bus lineal son de las más fáciles de instalar y son relativamente baratas. En esta topología una avería de una estación no afecta mas que a ella misma, pero una avería del bus afecta a toda la red. Tiene las ventajas de su modularidad y adaptabilidad a la distribución geográfica de las estaciones con costo reducido, lo que la hace ser la topología más sencilla. El cableado puede ser con coaxial, par trenzado o fibra óptica.

Los equipos conectados en red con esta topología transmiten datos a un equipo particular por el bus llegando los datos a todos los equipos en la red. La información solo es aceptada por el equipo cuya dirección coincida con la dirección incluida en la señal transmitida, los otros equipos no procesan los datos. Solo un equipo puede enviar sus datos cuando esta libre el bus. Cuanto más equipos haya conectados al bus, mas equipos estarán esperando para transmitir datos, por lo que la red será más lenta.

Como los datos o señales electrónicas transmitidas se envían a toda la red, es decir, viajan de un extremo a otro del cable, la señal puede continuar rebotando ininterrumpidamente una y otra vez por el cable provocando que otros equipos envíen señales, es por ello que la señal debe ser detenida una vez que llego a su destino. Para detener este rebote o eco de la señal el terminador en cada extremo del cable absorbe las señales libres, con lo cual libera al bus para que otros equipos puedan enviar datos. Si el cable es separado en dos o se desconecta un extremo del mismo, un extremo no tendrá un terminador por lo que la señal rebotara y la actividad de la red se detendrá.

Para realizar las transmisiones en la topología de bus, en cualquier instante una computadora es la maestra y puede transmitir, se pide a las otras maquinas que se abstengan de enviar mensajes. Para esto se utiliza un mecanismo de arbitraje para resolver conflictos cuando 2 o más maquinas quieren transmitir simultáneamente y de esta manera se evita que se genere el fenómeno llamado colisión. El mecanismo de arbitraje puede ser centralizado o distribuido, un ejemplo del mecanismo de arbitraje centralizado es el utilizado por la IEEE 802.3, más conocido como Ethernet, cuando se detecta una colisión

en el medio de comunicación las terminales involucradas dejan de transmitir un tiempo al azar, transcurrido ese tiempo lo intentaran de nuevo.
Las ventajas de la topología de Bus son:

- Es fácil de instalar y mantener, además que se pueden conectar nuevos nodos a la red fácilmente sin afectar el servicio.
- No existen elementos centrales de los que dependa toda la red cuyo fallo dejaría inoperativas a todas las computadoras.
- Comparado por ejemplo con la topología de estrella se requiere menos cable.

Sus desventajas son:

- Toda la red se cae si existiera una ruptura del cable backbone.
- Se requieren terminadores.
- Es un poco complejo determinar el origen de un problema cuando toda la red se cae.
- Los datos son recibidos por todas las estaciones por lo que se tiene que dotar a la red de un mecanismo para saber hacia que destinatario van los datos, y debido a que todas las estaciones pueden querer transmitir al mismo tiempo, se tiene que implementar un mecanismo para evitar que unos datos interfieran con otros. Para el primer problema se inserta en las tramas una información de control con el identificador de la estación destino y se mantiene una cooperación entre todas las estaciones mediante la información de control. Para el segundo caso se hace uso de los protocolos de contención o de acceso al medio.

Cuando se instala una red con la topología de Bus en un edificio con varias plantas, lo que se recomienda hacer es instalar una red de Bus por planta y después unirlas con un bus troncal.
Esta topología es muy usada con protocolos Ethernet.

- **Topología en Anillo**

En esta topología todas las estaciones están conectadas una con otra a un solo canal de comunicación por lo que es un sistema de difusión al igual que el de bus. En esta topología la conexión de las estaciones forma un anillo o circulo cerrado, Fig. 2.5.2.3.2.

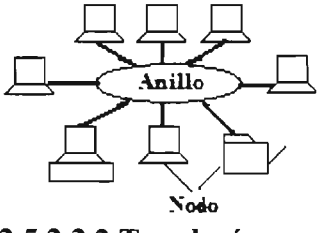


Fig. 2.5.2.3.2 Topología en anillo

Para formar este tipo de red se tienen una serie de repetidores que reciben y retransmiten en un solo sentido la información sin almacenarla. Cada estación se conecta al anillo con un repetidor que pasa la información de la red a la estación y viceversa.
Los datos circulan en el anillo en una sola dirección. En las tramas de información se incluye el identificador sobre la estación destino.
Cuando la trama llega al repetidor este lo copia y retransmite al siguiente repetidor en una dirección predeterminada, el repetidor analiza la trama y si esta dirigida para su estación de enlace se lo pasa y si no lo elimina. Para impedir que una trama de vueltas continuamente por el anillo se puede eliminar ya sea por el repetidor destino o por el repetidor origen

cuando le vuelve a llegar la trama. Los repetidores pueden estar en tres estados posibles: escucha, cuando recibe las tramas del anillo comprueba si pertenecen a su estación, si los son le pasa dichas tramas, sino los reenvía otra vez al anillo; transmisión, cuando el enlace tiene permiso para transmitir datos de su estación entonces los pasa al anillo y el ultimo estado de cortocircuito, el repetidor sin hacer la comprobación pasa la información otra vez al anillo.

Sus principales características son:

- El cable forma un bucle cerrado formando un anillo al cual se conectan todas las computadoras que forman parte de la red.
- Las redes en anillo usan como método de acceso al medio el modelo paso de testigo.

Desventajas de la topología de anillo

- Si se rompe un enlace o falla un repetidor el resto del anillo queda inservible paralizando toda la red.
- Es difícil de instalar.
- Cada vez que introduce un nuevo repetidor se tiene que adaptar a sus vecinos.
- Requiere mantenimiento.

- **Topología en Estrella**

En esta topología de red todas las estaciones de trabajo están conectadas mediante enlaces bidireccionales a un nodo central que asume las funciones de gestión y control de las comunicaciones proporcionando un camino entre dos dispositivos que deseen comunicarse, el nodo central normalmente es un dispositivo concentrador, Fig.2.5.2.3.3.

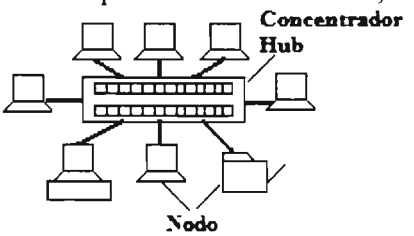


Fig. 2.5.2.3.3 Topología de estrella

El concentrador o hub controla todas las funciones de la red además de actuar como amplificador de los datos. Las estaciones se comunican unas con otras a través del nodo central, este puede funcionar de dos formas: el nodo solo repite y retransmite las tramas que le llegan hacia todas las demás en este caso la red funciona igual que la topología de bus; en la otra forma de funcionamiento el nodo central al llegarle la trama la almacena para usar el identificador de cada estación y los datos de destino y así transmitir la trama solamente al destino.

Esta configuración suele hacerse con cable de par trenzado aunque también es posible implementarla con cable coaxial o fibra óptica. La principal ventaja de esta topología es que la decisión de cuando una estación puede o no transmitir se halla bajo control central, además la flexibilidad en cuanto a configuración y localización de fallos es aceptable al estar toda la funcionalidad localizada en un nodo central. En esta topología si una de las estaciones de trabajo no funciona, no afecta a las demás, pero el nodo central es una fuente potencial de fallo que puede dejar inoperante la red si falla. Esta topología se puede usar tanto con el protocolo Ethernet como con LocalTalk.

Características de la topología en estrella:

- Todas las computadoras se conectan al punto central o concentrador formando una estrella física.
- Con esta topología se puede usar como método de acceso al medio el poleo, siendo el nodo central el que se encarga de implementarlo.
- Es muy fácil de instalar.
- Cuando dos computadoras se quieren comunicar la información transferida de una hacia otra debe pasar por el punto central.
- La velocidad es alta para la comunicación entre el nodo central y los nodos extremos, pero es baja entre los nodos extremos.
- Se pueden desconectar elementos de red sin causar problemas al resto de la red.
- Si falla un cable solo se pierde la conexión del nodo al cual interconectaba.
- Es más fácil detectar un fallo y repararlo.

Desventajas:

- Requiere mas cableado que la topología de Bus.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos conectados a el.
- Se tienen que adquirir equipos concentradores.

- **Topología en Árbol (Tree)**

La topología de árbol combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes en estrella conectadas a un bus, Fig. 2.5.2.3.4. Esta topología facilita el crecimiento de la red. El cableado a usar puede ser par trenzado, coaxial o fibra óptica. Se usa con el protocolo Ethernet.

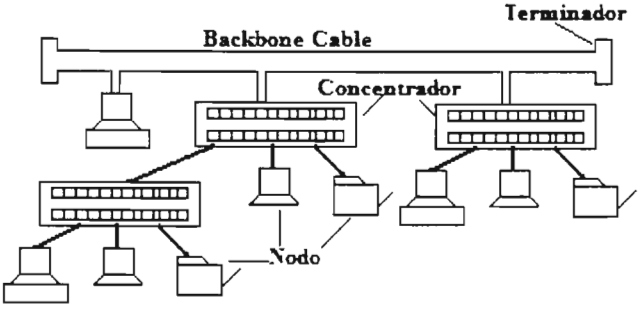


Fig. 2.5.2.3.4 Topología de Árbol

Ventajas de la topología de árbol

- El cableado es punto a punto para segmentos individuales.
- Soportado por muchos vendedores de software y hardware.

Desventajas

- La medida de cada segmento es determinada por el tipo de cable utilizado.
- Si falla el segmento principal toda la red falla.
- Es más difícil la configuración.

Esta topología de árbol también se puede implementar con una topología bus-estrella, la cual como centro tiene a un concentrador que implementa internamente al bus y al que

están conectadas todas las computadoras. La diferencia que existe entre esta topología lógica y la topología en estrella con hub es el método de acceso al medio que utiliza.

- **Topología lógica Anillo-estrella o Token Ring**

Uno de los inconvenientes de la topología en anillo era que si el cable se rompía, toda la red quedaba inoperativa, con la topología mixta anillo-estrella este y otros problemas quedan resueltos. Esta topología físicamente parece una topología estrella pero el tipo de concentrador utilizado, conocido como MAU (Multi-Station Access Unit) se encarga de interconectar internamente la red en forma de anillo, Fig. 2.5.2.3.5. El cableado se realiza con par trenzado.

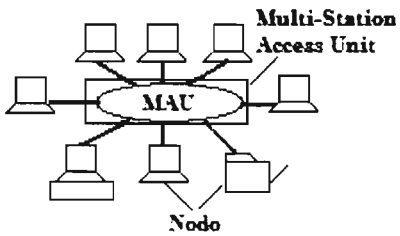


Fig.2.5.2.3.5 Topología anillo-estrella

Sus principales características son:

- Cuando se instala una configuración en anillo, el anillo se establece de forma lógica (internamente el equipo concentrador se constituye de un anillo), ya que de forma física se usa una configuración en estrella
- Se utiliza un concentrador o incluso un servidor de redes como dispositivo central, de esta forma si se daña algún cable solo queda inoperativo el nodo que conectaba y los demás pueden seguir funcionando.
- El concentrador que se utiliza es un MAU (Unidad de Acceso Multiestación) que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.
- Cuando la MAU detecta que un nodo se ha desconectado puentea su entrada y su salida para así cerrar el anillo.

Esta topología de anillo estrella (Star Wired Ring) se usa en redes con protocolo Token Ring.

Las redes Token Ring fueron el primer tipo de red LAN de tecnología IBM. Estas redes basadas en unos sistemas llamados Token Passing basan el control de acceso al medio en la posesión de un token. El token es un paquete físico especial (no es un paquete de datos) con un contenido especial que permite a la estación que lo posee realizar la transmisión. Cuando ninguna estación necesita transmitir, el token va circulando por la red de una a otra estación. Cuando una estación transmite cierta cantidad de información debe pasar el token a la siguiente. Cada estación puede mantener el token por un periodo limitado de tiempo, no más de 10 mseg. Las redes Token Ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para una velocidad de transmisión de 4 Mbits/s. Las de 16 Mbits/s no tienen alguna especificación asociada.

Clasificación por tecnología.
La clasificación por tecnología de transmisión se puede realizar en tres tipos básicamente:

- Topología por tecnología Ethernet (bus, estrella o árbol).
- Topología por tecnología Token Bus.
- Topología por tecnología FDDI.

- **Topología por tecnología Ethernet**

El protocolo ethernet se puede usar en tres tipos de redes con topología en Bus, estrella y árbol, Fig. 2.5.2.3.6:

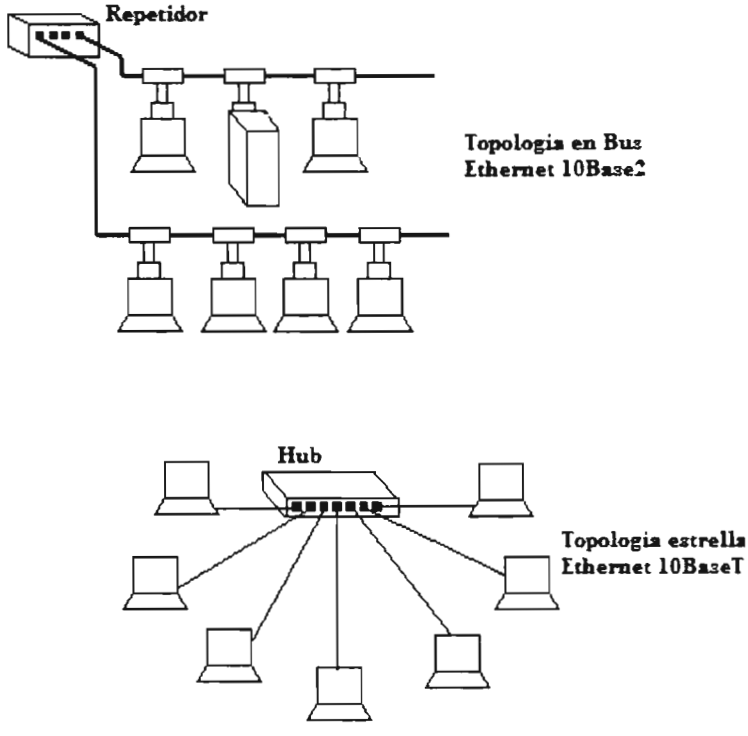


Fig. 2.5.2.3.6 Topología por tecnología ethernet

El funcionamiento de las dos topologías mostradas en la Fig. 2.5.2.3.6 es igual al explicado anteriormente en las topologías de bus y estrella, por su parte la topología en árbol es una combinación de varias topologías de estrella interconectadas por topologías en bus.

- **Topología Token Bus**

En esta topología los dispositivos están físicamente conectados a un bus (cable lineal) pero están organizados lógicamente en un anillo, Fig. 2.5.2.3.7.
El cableado de esta topología Token Ring puede ser con cable UTP o fibra óptica.

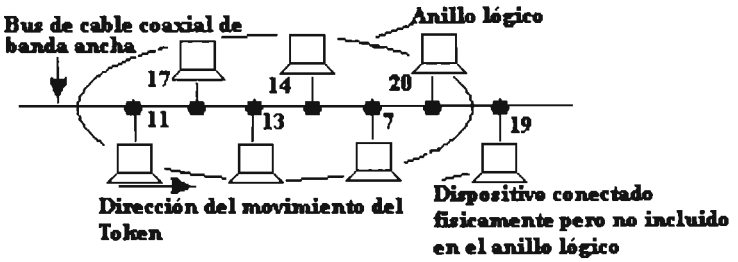


Fig. 2.5.2.3.7 Topología Token Bus

- **Topología FDDI**

La tecnología de interfase de datos distribuidos por fibra FDDI (Fiber Distribuited Data Interface), especifica una red token-passing de 100 Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 Km., FDDI utiliza una arquitectura de anillo doble para proporcionar redundancia., Fig. 2.5.2.3.8 a)

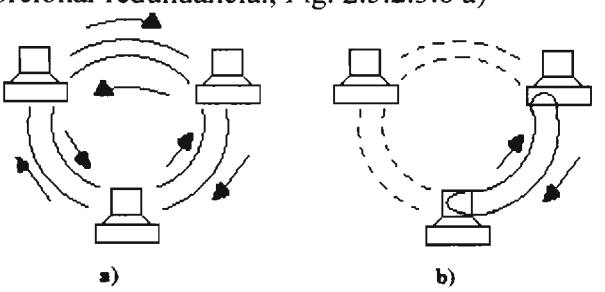


Fig. 2.5.2.3.8 Topología FDDI

El método de acceso al medio usado por FDDI se basa en el paso de testigo (token passing). En este tipo de redes la topología es de anillo dual. La transmisión se da en uno de los anillos, pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión. Los anillos se hacen con fibra óptica.

Factores a considerar en la selección de una tecnología de red.

Es importante seleccionar la topología mas adecuada a las necesidades existentes. Existen una serie de factores a checar al momento de decidirse por una topología de red:

- La distribución de los equipos a conectar
- Tipo de aplicaciones que se van a ejecutar
- El costo de la inversión que se realizara en los medios de comunicación
- Modularidad para poder determinar la sencillez de instalación y mantenimiento.
- La flexibilidad y capacidad de escalabilidad de la red, para poder incrementar él numero de conexiones a la red así como la complejidad que este incremento tenga.
- Costo del mantenimiento y actualización de la red local.
- El trafico que va a soportar la red local, determinando los retardos que provoque, así como el caudal para manejar grandes flujos de información sin que se produzcan bloqueos o congestiones.
- La confiabilidad que proporcionara la red cuando un elemento, como una estación o el medio de comunicación fallen.
- Capacidad de readaptación de la red para que cuando un componente falle se pueda reconfigurar para mantener el servicio por otro camino diferente.

2.5.3 Características, estructura y funcionamiento de las redes Lan

La estructura de una red de área local LAN requiere que las estaciones de trabajo individuales estén unidas físicamente por algún medio de transmisión, los más comunes son cable coaxial o par trenzado. También se necesita que haya algún software de red residente en disco duro que permita compartir periféricos, datos y programas de aplicaciones. Estas redes son de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales PCs y estaciones de trabajo en oficinas de las empresas con el objeto de compartir recursos e intercambiar información entre usuarios.
Como las LAN están restringidas en tamaño, sus tiempos de retransmisión están limitados y son conocidos por lo tanto pueden ser controlados sobre la base de diseños adecuados de la red.
Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo compartido al cual están conectadas todas las maquinas con sistemas de difusión (Broadcasting).
En una red local la información que se quiere transmitir es paquetizada por el protocolo usado para realizar la transmisión, en el paquete se agregara la dirección del nodo destino y la dirección del nodo origen, el paquete se transporta por los medios según las normas de los protocolos de comunicación establecidos. Si la información va dirigida a una red diferente la trama debe llegar a un dispositivo de interconexión de redes como un router. un gateway o un puente, los cuales decidirán el camino que debe seguir la trama.

Características de las redes LAN:

- Una red LAN permite compartir recursos tanto de hardware como de software.
- Mejora la productividad, la administración de la información, y la interacción entre el personal.
- Reduce y controla costos.
- Estandariza el uso de hardware y software.
- Utiliza medios privados de comunicación.
- Alcance. Las distancias que abarcan las redes LAN van desde los metros hasta unos pocos kilómetros.
- Velocidad. Las velocidades de transmisión son elevadas comparadas con las que normalmente se utilizan en una red de área extensa.
- Conectividad. Permiten la comunicación de igual a igual de los dispositivos conectados independientemente si son grandes procesadores o son computadoras personales.
- Interconexión. Ofrecen la posibilidad de conexión con otras redes mediante la utilización de gateways.
- Manejan un gran tráfico de información debido al mayor uso de la red y al mayor numero de usuarios.
- Se tienen aplicaciones muy demandantes de recursos como las intranets y las aplicaciones cliente-servidor.
- La tendencia es una migración hacia esquemas basados en la conmutación.
- Maneja trafico de multimedia.
- Existe gran predominancia de las tecnologías derivadas de Ethernet.

- En general una red LAN se caracteriza por el medio de transmisión utilizado para la interconexión de dispositivos, la topología, el método de acceso al medio que determina la forma en que los dispositivos de red pueden accesar al medio de transmisión y la técnica de transmisión que es la forma en que se envía la información al medio de comunicación.
- Una LAN es efectiva si cumple con las siguientes características:
  - Simplicidad
  - Confiabilidad
  - Transparencia
  - Facilidad de administración

Las ventajas de las redes LAN son:

- Altas velocidades de transmisión y baja cantidad de errores.
- Bajo costo.
- Alta confiabilidad e integridad.
- Flexibilidad de instalación.
- Facilidad de Expansión.
- Adaptabilidad de la aplicación.
- Interfaces estandarizadas.
- Compartimiento de recursos.

Desventajas:

- Numero de nodos conectados físicamente.
- Rendimiento de la red.

Las arquitecturas LAN referidas al Modelo OSI tienen en las dos primeras capas las siguientes funciones:

1. Capa física:
   - Codificación y decodificación de las señales.
   - Generación y eliminación de preámbulo.
   - Transmisión y recepción de bits.
2. Capa de enlace-Subcapa de Control de Acceso al Medio (MAC):
   - Ensamblado de datos en tramas con campos de direccionamiento y detección de errores.
   - Desensamblado de tramas, reconocimiento de direcciones y detección de errores.
   - Control de acceso al medio de transmisión LAN.
3. Capa de enlace-Subcapa de Control de Enlace Lógico (LLC):
   - Interfaz con las capas superiores y control de errores y de flujo.

Cada capa toma las tramas y le añade una serie de datos de control antes de pasarla a la siguiente capa, Fig. 2.5.3.1

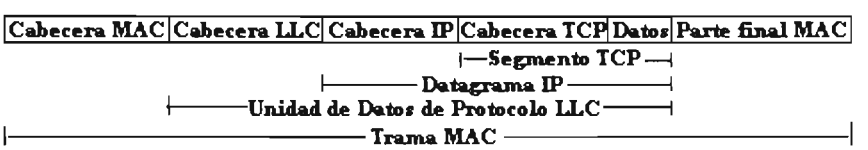


Fig. 2.5.3.1 Agregado de datos a la trama

1. Capa física:

En la capa física se realiza la codificación y decodificación de señales, la generación y transmisión del preámbulo y la transmisión y recepción de bits

La estructura de las redes LAN de tipo ethernet pueden ser de diferentes tipos según la norma de cableado IEEE 802.3 entre las cuales tenemos:

- 10Base5
  - El ethernet de cable coaxial grueso (Thick Ethernet) usa un cable especial de 50 ohms de impedancia en una estructura de bus, con una desventaja, si el coaxial es interrumpido en cualquier lugar, la red entera se caerá.
  - Se requiere un tranceiver para la traducción de señales entre el bus y la tarjeta adaptadora de red a través de un cable AUI (Atachment Unit Interface-Interfaz de Unidad de Conexión).
  - El bus debe ser terminado en ambos extremos con una resistencia de 50 ohms.
  - Utiliza un conector N sobre el coaxial (vampiro).
  - Los segmentos de cable no deben exceder de 500 m de longitud.
  - Habrá mínimo 2.5 m entre cada tranceiver
  - Máximo 100 usuarios por segmento.
  - La velocidad en el bus es de 10 Mbps.
  - Se puede usar en backbones de alta velocidad.

- 10Base2
  - El ethernet delgado (thin ethernet) usa un cable coaxial delgado (RG58) con una impedancia de 50 ohms.
  - Se instala en una estructura de bus.
  - El tranceiver o transductor esta incluido en la tarjeta adaptadora de red.
  - El bus debe tener un terminador en ambos extremos con una resistencia de 50 ohms.
  - Usa conectores BNC.
  - Los segmentos de cable deben tener una longitud máxima de 185 m.
  - Deberá tener al menos 0.5 m entre dos conectores T´s.
  - Máximo 30 usuarios por segmento.
  - La velocidad en el bus será hasta de 10 Mbps.

- 10BaseT
  - Es la versión en par trenzado de ethernet. El par trenzado puede ser del tipo UTP, FTP o STP.
  - La red se implementa en una topología en estrella en donde el concentrador es el centro del cableado. 10BaseT tiene físicamente una topología en estrella la cual es convertida a una estructura de bus Ethernet dentro del concentrador.
  - Usa un conector estandarizado RJ45 de 8 hilos.
  - Se usan solo los pares dos y tres del par trenzado para transmitir y recibir.
  - Hasta 100 m de distancia entre el hub y la terminal.
  - Hasta 1024 nodos por segmento.

- 10BaseFL
  - También conocido como el estándar FOIRL (Fiber Optic Inter Repeater Link) o ethernet sobre fibra óptica.
  - Normalmente usa fibras de 50/125 y 62.5/125 micrómetros de diámetro.
  - Se necesita un enlace dual de fibras (transmisión y recepción).
  - Comúnmente se usa para soportar estructuras de columna dorsal o Backbone.
  - La configuración es en estrella igual que 10BaseT.
  - El hub o concentrador consiste de un acoplador pasivo en estrella y retransmite todas las señales recibidas de las fibras ópticas a todos los puertos, para formar un segmento simple de fibra óptica.

2. Capa de enlace-Subcapa de Control de Acceso al Medio (MAC):

La subcapa MAC maneja el mecanismo encargado del control de acceso de cada estación al medio.
Las técnicas de la subcapa MAC pueden ser sincronas o asíncronas. Las sincronas no son recomendables para una red LAN ya que hacen que se comporte como una red de conmutación de circuitos. Las asíncronas son más recomendables puesto que las LAN actúan de forma impredecible. Estas técnicas asíncronas se dividen en 3 categorías: rotación circular, reserva competición.

- Rotación circular: se rota la oportunidad de transmitir a cada estación, si no se tiene nada que transmitir, se declina la oferta y se deja el paso a la siguiente estación. A la estación que quiere transmitir solo se le permite una cierta cantidad de datos en turno.
- Reserva. Esta técnica es adecuada cuando las estaciones quieren transmitir un largo periodo de tiempo, de modo que se reservan ranuras de tiempo para repartirse entre todas las estaciones.
- Competición. Todas las estaciones que quieren transmitir compiten para poder hacerlo (el control de acceso al medio se distribuye entre todas las estaciones).

3. Capa de enlace-Subcapa de Control de Enlace Lógico (LLC):

La subcapa LLC se encarga de transmitir las tramas entre dos estaciones sin pasar por ningún nodo intermedio, permite el acceso múltiple, e identifica todos los posibles accesos a ella, ya sean de una capa superior como estaciones destino u otros.

- Servicios LLC: la subcapa LLC debe controlar el intercambio de datos entre dos usuarios y para ello puede establecer ya sea una conexión permanente o una conexión cuando se requiera el intercambio de datos o una mezcla de estas.
- Protocolo LLC: hay varias formas de utilización de este protocolo que van desde envío de tramas con requerimiento de confirmación hasta conexiones lógicas entre dos estaciones previo intercambio de tramas de petición de conexión.

Funcionamiento de las redes LAN

Las redes locales se componen de un conjunto de dispositivos que comparte la capacidad de transmisión de la red a la que se encuentran conectados. Para evitar conflictos y errores se usan métodos de control de acceso al medio de transmisión. El protocolo de control de

acceso al medio es el factor que más caracteriza el funcionamiento de una red de área local. Los métodos de compartición mas utilizados son el CSMA/CD el cual pertenece a las técnicas de contienda y paso de testigo en anillo perteneciente a las técnicas controladas.

Método de compartición del medio controlado

Las técnicas de compartición controladas o Round Robin están basadas en la filosofía de conceder a cada uno una oportunidad. Cada estación por turno recibe el permiso de transmitir. Durante su oportunidad la estación puede declinar transmitir o bien transmitir sujetándose a ciertos limites generalmente expresados en cantidad máxima de tiempo. En cualquier caso la estación cuando finaliza, debe ceder su turno pasando el derecho de transmisión a la siguiente estación dentro de la secuencia lógica de estaciones. El control de turnos puede estar centralizado o distribuido. El sondeo o poleo es un ejemplo de técnica centralizada. Las técnicas de paso de testigo pertenecen al grupo de métodos distribuidos.

- Dentro de las técnicas de control centralizado tenemos la técnica de sondeo, la cual es más utilizada en redes WAN. Se fundamenta en la relación maestro-esclavo entre el nodo central y las demás estaciones.

En una topología de anillo, para que un nodo pueda transmitir debe recibir permiso del nodo central a través de un mensaje de sondeo. El permiso va pasando secuencialmente de estación a estación a lo largo de toda la red. La estación realiza su transmisión cuando recibe permiso, al finalizar su transmisión pasa su permiso a la siguiente estación. El inconveniente de esta técnica es que la comunicación entre dos nodos tiene que pasar por el central.

En la topología en bus, la estación central pregunta por turnos a cada estación subordinada si tiene algún mensaje para enviar, en caso afirmativo la estación subordinada recibe permiso para enviar la información a la estación central que a su vez la transmite hacia la estación destino. Durante esta transacción la estación subordinada también recibe los datos que pudieran estar destinados a ella. El mismo nodo para volver a transmitir ha de esperar a ser interrogado nuevamente.

Estos dos métodos no responden realmente a las necesidades de una red de área local mas bien se usaban para control de dispositivos.

- En las técnicas de control distribuido todas las estaciones de la red intervienen en la circulación de un paquete especial de información que recibe el nombre de testigo (token) y que indica a la estación que lo recibe que tiene a su disposición el medio para efectuar una transmisión, se aplica a las topologías de anillo y bus.

Paso de testigo en Bus (Token Bus).

Las estaciones del árbol o bus forman un anillo lógico, esto es, a las estaciones se les asigna una posición lógica en una secuencia ordenada y circular. Cada estación conoce la identidad de su estación antecesora y de su sucesora en el anillo lógico, el arreglo físico de las estaciones en el bus es irrelevante e independiente del orden lógico. La Fig. 2.5.3.1 es una muestra de la técnica, las estaciones B a G están inscritas en el anillo por donde circula el testigo por lo que pueden enviar y recibir información. Las estaciones A y H están excluidas y no pueden enviar información sin embargo pueden seguir recibiéndola por las características de difusión de la topología física en bus.

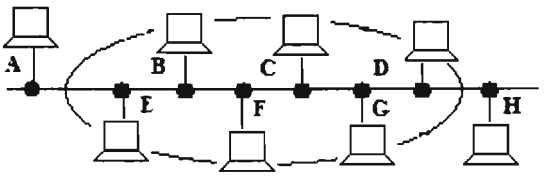


Fig. 2.5.3.1 Paso de testigo en bus

Como se ha indicado una trama de control, testigo o token, regula el derecho de acceso al medio para transmitir. Una vez finalizada su transmisión o expirado el tiempo asignado la estación que lo posee pasa el testigo a la estación siguiente en la secuencia lógica. El estado normal de operación es una alternancia de fases de transferencia de información y transferencia de testigo. En ésta técnica se requieren funciones de mantenimiento, por lo cual una o más estaciones realizan las siguientes funciones:

- Iniciación del anillo. Cuando se arranca la red o se recupera de un fallo de funcionamiento, el anillo debe iniciarse, para esto se necesita un algoritmo descentralizado que decida el orden de iniciación.
- Adición al anillo. Periódicamente debe concederse la oportunidad a las estaciones no participantes de insertarse en el anillo.
- Eliminación del anillo. Una estación debe ser capaz de retirarse del anillo.
- Recuperación de errores. Esto se tiene que realizar cuando se tienen direcciones duplicadas o roturas del anillo.

Paso de testigo en anillo (Token Ring).

Esta técnica al igual que la de paso de testigo en bus, se basa en una pequeña trama, testigo o token que circula a lo largo del anillo. Un bit indica su estado: libre u ocupado, Cuando ninguna estación transmite, el testigo simplemente circula por el anillo pasando de una estación a la siguiente. Una estación que desee transmitir debe esperar a recibir el testigo, entonces modifica el estado del testigo de libre a ocupado e inserta a continuación la información a enviar junto con su propia dirección y la de la estación destino. El paquete de datos así modificado prosigue su circulación por el anillo hasta llegar a la estación receptora que copia su contenido y lo vuelve a poner en circulación. Cuando el paquete vuelve a llegar a la estación emisora, esta lo retira de la red y genera un nuevo testigo libre.

Método de compartición del medio por contienda.

Las técnicas de acceso aleatorio o contienda, son aleatorias en el sentido de que no es predecible cuando va a transmitir una estación, son de contienda por que no existe un control que determine el orden de transmisión, todas las estaciones deben competir por el derecho de acceso.

El primer método de acceso aleatorio fue conocido como transmisión sin escucha, llamado ALOHA puro, el cual fue desarrollado para la comunicación de terminales dispersos con una computadora central vía satélite aunque es aplicable a cualquier medio de transmisión compartido. El protocolo es simple, se transmite el mensaje en cuanto hay uno preparado para ello. A continuación la estación escucha el medio durante un periodo de tiempo igual al doble del tiempo de propagación entre las dos estaciones mas separadas, si se recibe reconocimiento de la transmisión todo ha salido bien de lo contrario se reenvía la trama. Después de repetidos intentos se aborta la transmisión.

Otra técnica de acceso aleatoria es la transmisión con escucha o acceso múltiple con detección de portadora (CSMA Carrier Sense Multiple Access) también conocida como escuchar antes de hablar (LBT Listen Befote Talk). Una estación que desee transmitir, escucha primero el medio para determinar si hay otra transmisión en progreso. Si es así la estación tras un periodo de espera lo vuelve a intentar siguiendo un algoritmo. Si el medio esta libre la estación transmite, puede suceder que dos o más estaciones intenten transmitir casi al mismo tiempo. Se producirá en este caso una colisión. Para tratar esta situación tras transmitir, la estación espera la confirmación durante un periodo de tiempo teniendo en cuenta el retardo máximo de propagación de la red y el hecho de que la estación que tiene que emitir la confirmación debe competir por el canal para responder. Si no hay confirmación la estación emisora asume que se ha producido una colisión y retransmite.
En la técnica CSMA hay dos algoritmos que son los más usados para especificar lo que debe hacer una estación si encuentra el medio ocupado. La primera es el algoritmo CSMA no-persistente en el que la estación que desea transmitir escucha el medio y sigue las siguientes reglas:

1) Si el medio esta libre, transmite
2) Si el medio esta ocupado, espera durante un periodo de tiempo extraído de una distribución de probabilidad y vuelve al paso 1.

La utilización de tiempos de retransmisión aleatorios reduce la probabilidad de colisiones, la desventaja es que aunque haya varias estaciones preparadas para transmitir es probable que haya un periodo de tiempo durante el cual el medio permanece ocioso después de una transmisión.
Para evitar este periodo de inutilización se emplea el protocolo l-persistente. En este caso la estación que quiere transmitir escucha el medio y:

1) Si el medio esta libre transmite
2) Si el medio esta ocupado continua escuchando hasta que este disponible, entonces transmite inmediatamente.
3) Si se produce una colisión, reconocida por la inexistencia de confirmación, espera durante un periodo de tiempo aleatorio y vuelve al paso 1.

La técnica CSMA presenta una gran ineficiencia, cuando dos tramas se colisionan, el medio permanece sin utilizar, mientras dura la transmisión de las tramas afectadas. En el caso de tramas largas en comparación con el tiempo de propagación, la cantidad de ancho de banda desperdiciada es considerable. Es posible reducir este tiempo de ociosidad del medio si la estación se mantiene escuchando el canal mientras trasmite (detección de colisión), así se añaden las siguientes reglas a las de CSMA:

1) Si se detecta una colisión durante la transmisión, esta cesa inmediatamente y se trasmite una pequeña trama de consenso de colisión (trama de jam) para asegurarse de que todas las estaciones se han enterado de la existencia de la colisión.
2) Después de emitir la señal de jam se intenta transmitir, tras esperar un periodo de tiempo aleatorio, usando de nuevo CSMA.

Esta operación es la técnica conocida como CSMA/CD.

Método de acceso para redes de alta velocidad FDDI
El estándar FFDI a 100 Mbps surgió por la necesidad de interconectar computadores a muy alta velocidad. El método de control de acceso se defino para una topología en anillo, utilizando el principio del paso de testigo: solamente la estación que tiene el testigo puede transmitir. FDDI utiliza una topología con doble anillo. Con este doble anillo se puede

continuar la operación con todas las estaciones en caso de avería de un enlace. La diferencia fundamental con la técnica de paso de testigo en anillo convencional utilizando el estándar IEEE 802.5 es que en FDDI cuado una estación ha terminado de transmitir sus tramas libera un testigo con lo cual pueden existir simultáneamente múltiples tramas de distintas fuentes, si bien solo puede haber un testigo libre.
En este tipo de contienda un nodo es libre de mandar sus mensajes en cualquier momento sin estar seguro de que ningún otro dispositivo esta intentando transmitir simultáneamente. Cuando dos o más estaciones intentan ocupar el canal al mismo tiempo se produce una colisión entre los mensajes que están siendo transmitidos. Inmediatamente se ejecuta un proceso o algoritmo de contienda para resolver la posesión del medio. Los métodos de contienda pueden clasificarse en técnicas con o sin escucha (transmisión sorda) según si posee o no información del canal libre u ocupado. Normalmente esta escucha se efectúa por detección de la presencia de la señal, usando las técnicas de Acceso Múltiple con detección de portadora CSMA.

Actualmente entre las redes LAN predomina la tecnología Ethernet. Las redes Ethernet por ser redes de difusión usan una técnica para que el dispositivo que desea transmitir tome su turno y evite de esta forma la colisión de paquetes de información en la red, para esto se usa el protocolo de acceso múltiple con senso de portadora y detección de colisiones CSMA/CD (Carrier Sense Múltiple Access/Collision Detección) sobre la base del funcionamiento de este protocolo se pretende explicar en cierta forma el funcionamiento de las redes LAN:

- Todos los componentes de la red (servidores estaciones de trabajo, dispositivos de interconexión, Etc.) se conectan a un cable coaxial que es el medio de transmisión, este cable se conoce como ether.
- Cuando la interfaz de red del componente de red tiene un paquete para transmitir, escucha el ether para determinar si hay mensajes siendo transmitidos.
- Si no detecta transmisión alguna, la interfaz comienza a enviar su información.
- Cada transmisión esta limitada en el tiempo, pues existe un tamaño máximo de paquete.
- Cuando un nodo comienza a transmitir, la señal no llega a cada punto de la red simultáneamente, a pesar de que viaja a casi un 80% de la velocidad de la luz.
- Por lo anterior es posible que 2 nodos determinen que la red esta ociosa y comiencen a transmitir al mismo tiempo, provocando la colisión de las dos señales.
- Detección de colisiones: Cada nodo monitorea el cable mientras esta transmitiendo para verificar que una señal externa no interfiera con la suya.
- Cuando una colisión es detectada la interfaz aborta la transmisión y espera hasta que la actividad cese antes de volver a intentar la transmisión
- Política de retención exponencial. El emisor espera un tiempo aleatorio después de la primera colisión; un periodo de espera 2 veces mas largo que el primero en caso de una segunda colisión; 4 veces más largo la próxima vez, y así sucesivamente, reduciendo de esta manera la probabilidad de colisión.

Este funcionamiento de ethernet o IEEE802.3 es implementado en el hardware de la tarjeta de interfaz de una computadora.

2.5.3.1 Medios de transmisión de las redes Lan

El medio físico que transporta información es un aspecto importante a tener en cuenta cuando se diseña e instala una red de área local, ya que este puede condicionar la distancia, velocidad de transmisión, topología e incluso el método de acceso a la red. Los principales medios de transmisión utilizados en las redes de área local son el cable de par trenzado, el cable coaxial y el cable de fibra óptica, así como los enlaces de radio para las redes inalámbricas, estos los podemos clasificar de la siguiente forma:

- Los medios guiados que son los cables o medios de transmisión físicos
- Los medios no guiados o medios inalámbricos.

2.5.3.1.1 Medios físicos o guiados

Los medios guiados son los que utilizan un medio sólido por el cual realizan la transmisión de la información, estos medios sólidos principalmente son los cables.

Cables

El medio mas utilizado para formar una red es el cable. El cable es el medio a través del cual fluye la información a través de una red. Hay distintos tipos de cable que se pueden utilizar en las redes LAN, aunque el tipo de cable esta sujeto a la topología de la red, el tipo de red que se utiliza y el tamaño de esta. La configuración física para el cableado de interconexión de terminales es del tipo bus compartido.

Los tipos de cable mas usados en las redes LAN son:

- Cable de par trenzado sin apantallar UTP (Unshielded Twisted Pair).
- Cable de par trenzado apantallado STP (Shielded Twisted Pair).
- Cable coaxial.
- Cable de fibra óptica.

- **Cable de par trenzado.**

El cable de par trenzado por su bajo costo y sencillez de instalación es el medio mas utilizado en las comunicaciones tanto analógicas como digitales.

Estos cables se componen de pares de hilos trenzados, algunos están cubiertos con mallas protectoras para eliminar las interferencias electromagnéticas, el trenzado elimina las interferencias entre cables cercanos. Pueden transmitir analógica o digitalmente y su ancho de banda dependerá de la sección de cobre utilizado y la distancia que tenga que recorrer.

El cable de par trenzado puede ser apantallado STP (Shielded Twisted Pair) o sin apantallar UTP (Unshielded Twisted Pair).

- **Cable UTP**

Es un cable compuesto de 8 hilos de cobre forrados individualmente por una cubierta de plástico que es de color diferente para cada cable, los 4 pares de hilos se encuentran forrados por una cubierta plástica que forma en si el cable, cada par esta trenzado para evitar los ruidos, la emisión y la recepción de interferencia electromagnética. La relación de torque de cada par es diferente así la señal de cada par no se interfiere con la de los otros pares dentro del mismo cable.

El cable UTP es él mas utilizado por su bajo costo y sencillez de instalación. Manejan velocidades muy elevadas con longitudes de cable no superiores a 100 m.
Es el tipo de cable mas utilizado y es la mejor opción para pequeñas y medianas empresas. La calidad de este cable y la cantidad de datos que transmite varía en función de la categoría del cable. Las categorías van desde el cable de teléfono que solo transmite la voz humana hasta el cable categoría 5 capaz de transmitir 100 Mbps, la tabla 2.5.3.1.1.1 muestra las distintas categorías de cable.

Tipo	Frecuencia	Uso
Categoría 1		Voz (Cable de teléfono)
Categoría 2		Datos a 4 Mbps (LocalTalk)
Categoría 3	16 Mhz	Datos a 10 Mbps (Ethernet)
Categoría 4	20 Mhz	Datos a 16/20 Mbps Token Ring
Categoría 5	100 Mhz	Datos a 100 Mbps (Fast Ethernet)
Categoría 5e	100 Mhz	Datos hasta 1000 Mbps
Categoría 6	200 Mhz	Datos a 1000 Mbps (Gigabit Ethernet) y más
Categoría 7	600 Mhz	No estandarizado

Tabla 2.5.3.1.1.1 Categorías de cable UTP

La velocidad de transmisión de los cables depende de las categorías normalizadas por la EIA/TI, estas categorías son:

- Categoría 1: Es el hilo telefónico trenzado para calidad de voz, no puede usarse para datos. Su velocidad de transmisión es de 1 Mbps.
- Categoría 2: son los cables más sencillos y se utilizan para transmisión de datos a bajas velocidades. Su velocidad de transmisión es de hasta 4 Mbps.
- Categoría 3: Esta categoría comenzó utilizándose en redes Ethernet a 10 Mbps, con longitudes de segmento no superiores 100 m y máxima longitud de red de 500 m. Es el tipo de cable usado para implementar las redes Ethernet 10BaseT. Su uso se extendió a otro tipo de redes como paso de testigo a 4 Mbps y 16 Mbps y redes de alta velocidad de 100 Mbps pero utilizando los 4 pares de hilos.
  Esta categoría reúne los requerimientos básicos de cableado para telecomunicaciones. Maneja todas las aplicaciones para datos como ethernet. Los cables y conectores de equipo tienen parámetros de transmisión caracterizados hasta 16 Mhz.
- Categoría 4: Su velocidad de transmisión llega a 16 Mbps. Esta categoría no es muy utilizada.
  Todos los componentes son probados para un funcionamiento eléctrico de hasta 20 Mhz. Los cables poseen buena separación diafónica. Maneja todas las aplicaciones para datos como Token Ring/Ethernet.
- Categoría 5: Puede transmitir datos hasta 100 Mbps y 150 Mbps empleando normalmente solo dos pares de hilos.
  Los Cables y conectores de equipo tienen parámetros de transmisión caracterizados hasta 100 Mhz. Maneja aplicaciones como ATM y Fast Ethernet.
  Es el cableado que se utiliza en la actualidad sistema UTP CAT5.
- Categoría 6: Puede transmitir datos hasta 1000 Mbps.

Los cables y conectores de equipo tienen parámetros de transmisión caracterizados hasta 200 Mhz.
Maneja todas las aplicaciones como ATM y Gigabit Ethernet.
Es el sistema UTP CAT6 de mejor rendimiento disponible en la actualidad, pero es difícil encontrarlo en el mercado..

La diferencia entre las categorías es la tirantez, a mayor tirantez se tendrá mayor capacidad de transmisión de datos. Para conectar el cable UTP se usan conectores RJ45 (Register Jack).

- **Cable STP**

Es un cable de par trenzado con forro metálico por cada par separado, un forro externo de PVC cubre a todos los pares en su conjunto, impedancia de 150 ohms. Este cable es igual al cable UTP pero se le agrega un apantallamiento para proteger la transmisión de datos de las interferencias eléctricas.
Todos los componentes son probados para un funcionamiento eléctrico de hasta 350 Mhz.
Por su menor sensibilidad a las interferencias y menor atenuación el cable STP es muy adecuado para grandes distancias y altas velocidades de transmisión, puede operar en entornos de mucha interferencia.
Adecuado para aplicaciones de multimedia (simultáneamente video, voz y datos) y aplicaciones para datos superiores a 100 Mbps o ambientes industriales ruidosos.
Este tipo de cable tiene un costo elevado y por ser más gruesos son difíciles de instalar, por lo que únicamente se utilizan en instalaciones muy puntuales que requieren una calidad de transmisión muy alta.
Es muy usado en redes con topología Token Ring.

- **Cable FTP (Foil Screen Twisted Pair)**

El cable de par trenzado con doble forro metálico es un cable preparado para tener una eficiencia de protección electromagnética mejorada, forro externo de PVC, impedancia de 100 ohms.
Todos los componentes son probados para un funcionamiento eléctrico de hasta 300 Mhz.
Adecuado para aplicaciones de multimedia (simultáneamente video, voz y datos) y aplicaciones para datos superiores a 100 Mbps o ambientes industriales ruidosos.

- **Cable coaxial**

El cable coaxial se compone de un conductor de cobre en el centro envuelto en un aislante de teflón que lo separa de un apantallado metálico con forma de rejilla para aislar al cable de interferencias externas y a su vez todo el conjunto esta envuelto por un forro protector.
El cable coaxial tiene normalmente un mayor ancho de banda que el cable de par trenzado, es muy usado para señales de video y transmisiones de telefonía y datos de alta velocidad a distancias de varios kilómetros.
La instalación de este cable es mas complicada que la del UTP, pero gracias a su apantallado tiene un alto grado de resistencia a las interferencias, además que se pueden alcanzar distancias mayores que con los cables de par trenzado.
En redes Ethernet su utilización ha sido más extendida.
En redes de área local, el cable coaxial se emplea tanto para transmisión en banda base como para transmisión en banda ancha, la primera modalidad es la más usada frecuentemente.

La especificación de las redes tipo Ethernet para este cable usa una notación compuesta de tres parámetros vel.-TipodeTransmisión-distancia como 10-Base-2:
[Velocidad en Mbps] [Tipo de transmisión][Distancia en centenares de metros]
Donde:

- El primer parámetro indica la velocidad de transmisión en Mbps.
- El segundo parámetro indica si la transmisión es en banda base (sin modulación) o en banda ancha (con algún tipo de modulación).
- El tercer parámetro que se multiplica por 100 indica la longitud del segmento en metros.

Coaxial fino para transmisión en banda base
Existe el coaxial fino (thin coaxial) al que también se le llama thinet o 10Base2 que hace referencia a una red de tipo ethernet con coaxial fino en el cual la distancia máxima del mayor segmento es de 200 metros, reducido a 185 m en la práctica. Este tipo de cable es muy popular en las redes con topología de Bus.
Coaxial grueso para transmisión en banda base
También tenemos el cable coaxial grueso, thicknet o 10Base5, que se refiere a una red tipo ethernet con coaxial grueso en el que la mayor distancia posible es de 500 metros. Por sus características de protección son una buena opción en redes de bus extensas, aunque es un cable muy difícil de doblar.
En las señales de banda base la señal se transmite sin modulación. Así cada vez que se realiza una transmisión se utiliza todo el ancho de banda del medio, por lo que se tienen que usar técnicas de acceso a medio compartido para que este pueda ser usado por múltiples estaciones. La ventaja de este tipo de transmisión es su sencillez ya que no requieren moduladores ni demoduladores. La señal es transmitida al medio en forma de trenes de bits con lo que si se presentan secuencias de 1 o 0 continuas no habrá transiciones de la señal dificultando la sincronización entre el emisor y el receptor por lo que se utiliza mucho la codificación Manchester para producir transiciones en el flujo de bits.
Las características de los tipos de cable coaxial mas comúnmente empleados son mostradas en la tabla 2.5.3.1.1.2

Cable	Características
10-Base-5	Cable coaxial grueso (ethernet grueso) Velocidad de transmisión: 10 Mbps Tipo de transmisión Banda Base Longitud del segmento: máx. 500 m. Impedancia característica 50 ohms Conector tipo N
10-Base-2	Cable coaxial fino (ethernet fino) Velocidad de transmisión: 10 Mbps Tipo de transmisión Banda Base Longitud del segmento máx. 185 m. Impedancia característica 50 ohms Conector tipo BNC
10-Broad-36	Cable coaxial de banda ancha Velocidad de transmisión: 10 Mbps Tipo de transmisión Banda ancha Longitud del segmento 3600 m Impedancia 75 ohms Longitud máxima extremo a extremo de 3600 metros Longitud de un extremo es de 1800 metros
100-Base-X	Fast Ethernet Velocidad de transmisión 100 Mbps. Tipo de transmisión Banda base

Tabla 2.5.3.1.1.2 Características del cable coaxial

Características del cable coaxial de banda base:
- Es un medio muy usado en redes LAN.
- Las señales en las redes LAN son digitales y codificadas con el código Manchester. El espectro en frecuencias es totalmente utilizado por lo que no se puede realizar multiplexación de frecuencias.
- La transmisión es bidireccional.
- La longitud del cable es inversamente proporcional a la velocidad que pueden alcanzar las señales.

Características del cable coaxial de banda ancha:
- Usan señalización analógica. Permiten la multiplexación de frecuencias, por lo que en el mismo cable se pueden establecer varias conexiones. La distancia permitida es muy superior a la banda base ya que las señales analógicas alcanzan mas espacio con menos interferencia y atenuación.
- En modo normal este cableado solo permite transmisión unidireccional, por lo que para usar intercambios bidireccionales de información, se necesitan dos cables de red, uno de ida y otro de vuelta.
- Para permitir que por un mismo cable se transmitan señales en ambos sentidos, se puede hacer que las señales en una dirección se envíen en una gama de frecuencias y en la dirección opuesta en otra gama de frecuencias.

El conector para el cable coaxial es el BNC (Bayote-Neill-Concelman) que puede ser de tres tipos: normal, terminadores y conectores en T.

- **Fibra óptica**

El cable de fibra óptica es el medio de transmisión de mayor potencial para redes de alta velocidad.
Es un medio de transmisión de luz (por lo que no le afectan las interferencias), esta formado por dos cilindros coaxiales de vidrio transparentes y diámetros muy pequeños, el cilindro interior es el núcleo, esta hecho de fina fibra de vidrio (silicio) transparente capaz de conducir en su interior la energía óptica y el cilindro exterior es la envoltura de otro tipo de vidrio con diferente índice de refracción, el índice de refracción del núcleo es mayor que el de la envoltura. Este medio de comunicación es muy usado para la conexión de redes entre edificios por su inmunidad a la humedad y a la exposición solar.
El sistema de transmisión óptica tiene tres componentes:

- Transmisor de energía óptica con un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones), que se emiten a través de la fibra óptica. La fuente luminosa pueden ser semiconductores como el LED o rayos láser con una mayor capacidad.
- La fibra óptica que se conecta a la fuente luminosa y al detector de energía óptica.
- Detector de energía óptica.

Los rayos ópticos que se transmiten a través del núcleo tienen un cierto ángulo con respecto al eje de este. Al cabo de una cierta distancia los rayos ópticos alcanzan el revestimiento en el que se refractan, siguiendo la ley de Snell que establece que los senos de los ángulos de refracción son inversamente proporcionales a la velocidad de propagación de la luz en cada uno de los medios, la cual a su vez es proporcional al índice de refracción n, n=V/C, siendo V la velocidad de propagación en el medio y C la velocidad de propagación en el vacío. Cuando el ángulo de refracción en el material con el índice de refracción mas elevado alcanza un determinado valor no se produce refracción y toda la energía óptica se refleja. El ángulo de incidencia en el que se produce este fenómeno se conoce como ángulo critico. Para ángulos mayores hay reflexión y para ángulos menores refracción. Por lo tanto para que la energía óptica se refleje en el revestimiento y no atraviese este, el índice de refracción del núcleo debe ser mayor que el del revestimiento y los rayos deben alcanzar este con un ángulo superior al crítico con respecto a la perpendicular al eje del núcleo. De esta forma el rayo luminoso se propaga a través del núcleo, reflejándose en la frontera con la cubierta sin penetrar en el material de esta. Este funcionamiento se aplica a los dos modos de transmisión: el multimodo con índice escalonado y el multimodo con índice gradual. Para generar estos rayos ópticos se usa el LED.
En un tercer modo de transmisión, el llamado monomodo, los ángulos son críticos para que los rayos lleguen al destino sin reflexión, para esto se usa una luz coherente generada con láser a la vez que se reduce el tamaño del núcleo de 50 a 10 micras, con lo que las distancias y velocidades alcanzadas son superiores, condicionadas por la dispersión cromática. Las principales características de la fibra óptica son:

- Ancho de banda muy elevado.
- Pequeño tamaño y ligereza.
- Baja atenuación.
- Aislamiento electromagnético.

La fibra óptica puede transmitir señales a distancias mucho mayores que con cables coaxiales o par trenzado, además la cantidad de información que puede transmitir es mayor, se hace referencia a este cableado como 10BaseF lo que significa que es una red Ethernet que trabaja a una velocidad de 10 Mbps con la señal sin modular en un medio de transmisión o cableado de fibra óptica.
La velocidad de transmisión es muy alta desde 10 Mbps hasta 500 Mbps en algunas instalaciones especiales y no es afectada por interferencias. Los cables de fibra óptica se pueden usar en muchas aplicaciones en las comunicaciones de datos:

- Para conexiones locales entre ordenadores y periféricos o equipos de control y medición.
- Interconexión de ordenadores y terminales mediante enlaces dedicados de fibra óptica.
- Enlaces de fibra óptica de larga distancia y gran capacidad.

El cable de fibra óptica tiene muchas ventajas sobre el de cobre como son: el recorrido de la fibra a la velocidad de la luz $3x10^9$, su gran capacidad de transmisión de datos, inmunidad al ruido, menor atenuación y errores, bajo peso, mayor flexibilidad, soporte de amplia gama de temperaturas.
Su gran desventaja es no se puede conectar tan fácilmente un nuevo nodo en la red con solo insertarlo en el cable, el proceso de conectorización de la fibra es un poco complejo y delicado.
Los segmentos del cable de fibra óptica son de 2000 metros.
Los conectores para fibra óptica mas usados son el ST, tienen una apariencia similar a los conectores BNC. Actualmente se están usando con más frecuencia los conectores SC de uso más fácil y seguros que permiten que la conexión del cable de transmisión y recepción se haga de una sola forma y que no queden cruzados.

En la tabla 2.5.3.1.1.3 tenemos una comparación de los tres tipos de cable en cuanto a la distancia máxima de los segmentos de cable.

Especificación	Tipo de cable	Longitud máxima
10BaseT	UTP	100 metros.
10Base2	Thin coaxial	185 metros
10base5	Thick coaxial	500 metros
10BaseF	Fibra Óptica	2000 metros

Tabla 2.5.3.1.1.3 Tabla comparativa de los cables usados en redes LAN.

La norma IEEE 802.3 especifica una familia completa de sistemas de cableado como muestra la tabla 2.5.3.1.1.4

Características	10base5	10base2	10baseT	10baseFL	100baseT	10broad36	1000baseT
Tasa de datos	10	10	10	10	100	10	1000
Distancia máx.	500	185	100	2000	100	1800	100
Medios	Coaxial 50 Ω	Coaxial 50 Ω	UTP	FO	UTP	Coaxial 75 Ω	UTP
Topología	Bus	Bus	Estrella	Punto a punto	Bus	Bus dual	Bus

Tabla 2.5.3.1.1.4 Tabla de medios de transmisión según la norma IEEE 802.3

10Base5
En esta especificación se emplea un cable coaxial de 50 ohms de impedancia que permite alcanzar una velocidad de transmisión de la red de 10 Mbps utilizando señalización digital con codificación Manchester. Con estos parámetros la longitud máxima del segmento de red es de 500 metros. El cable coaxial de 50 ohms es un cable de uso específico utilizado generalmente en las redes locales de banda base y topología en bus. Con este cable la señal digital experimenta reflexiones mas reducidas cuado se insertan las derivaciones. También experimenta mayor inmunidad contra el ruido de baja frecuencia.

10Base2
La especificación 10Base2 también utiliza un cable coaxial de 50 ohm y codificación Manchester a una velocidad de 10 Mbps. Este cable coaxial es más delgado, más flexible y más fácil de doblar. La longitud máxima del segmento es de 185 metros.

10BaseF
10BaseF es una especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BaseFB, 10BaseFL y 10 BaseFP para ethernet a través de cableado de fibra óptica

10BaseT
10BaseT es una especificación ethernet de banda base de 10 Mbps que utiliza la codificación Manchester, tiene un limite de distancia aproximado de 100 metros por segmento. Esta especificación define una topología física en estrella y topología lógica de bus, utiliza dos pares de cable de par trenzado (categorías 3, 4 o 5): un par para transmitir datos y el otro para recibir datos, los cuales se conectan a un punto central y este elemento central retransmite la señal que le llega hacia las demás estaciones, el dispositivo central es un repetidor multipuerto también llamado hub o concentrador.

100BaseT
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la cual se basa 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico. Sin embargo estos impulsos contienen más información que los utilizados en 10BaseT. Esta basado en el estándar IEEE 802.3.

100BaseTX
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares del cableado UTP o STP. El primer par de cables se emplea para recibir datos y el segundo para transmitir. Para garantizar una correcta temporización de las señales un segmento 100BaeTX no puede exceder los 100 metros de longitud. Se basa en el estándar IEEE 802.3

10Broad36
Es una especificación para banda ancha. El medio empleado es el cable coaxial CATV de 75 ohms utilizado para las antenas de televisión, su longitud máxima es de 1800 metros, teniendo en cuenta la topología bus dual utilizada, la longitud máxima extremo a extremo es de 3600 metros. La velocidad de transmisión es de 10 Mbps.

Factores que se deben tomar en cuenta cuando se elige un cable como medio de comunicación de una red:

- Ancho de banda. El ancho de banda esta definido por el espectro de frecuencias que el medio puede transferir, cuanto mayor es el ancho de banda se pueden obtener velocidades de transmisión mas elevadas.
- Distancia máxima entre los ordenadores que se van a conectar. Esta distancia será determinada por la longitud de un segmento de cable el cual es función del tipo de cable, arquitectura y topología de la red. Para cada arquitectura y tipo de cable se definen distancias máximas alcanzables.
- La fiabilidad en la transferencia de la información determina la calidad de la transmisión, se evalúa con el porcentaje de errores por número de bits transmitidos. Se relaciona con la atenuación así como la sensibilidad al nivel de ruido e interferencias habituales en la zona que se va a instalar la red.
- Seguridad. Indica el grado de dificultad con que las señales transportadas pueden ser interceptadas.
- Facilidad de instalación. Se relaciona con la ligereza y diámetro del cable, así como su sensibilidad para los trabajos que sobre el se realicen. Por ejemplo la instalación y ajuste de los optoacopladores para la fibra óptica es muy complejo.
- El costo es un aspecto determinante en la selección del cable. El más económico es el par trenzado y la fibra óptica es la más costosa.

2.5.3.1.2 Medios no físicos o no guiados

Los medios no guiados son los que utilizan el aire para transmitir los datos por ello son llamados también medios inalámbricos.

Las redes pueden ser implementadas sin la necesidad de tener que estar conectadas las estaciones con cableado. En redes LAN se tienen también medios no físicos para realizar la transmisión y comunicación entre los elementos que integran la red. Se pueden utilizar señales de alta frecuencia o haces infrarrojos para comunicarse. Cada nodo de la red puede usar una antena desde la que emite y recibe señales.

El uso de este tipo de conexión sin cableado es especialmente útil para equipos portátiles o para su instalación en edificios que no tengan las condiciones para instalar un cableado o simplemente por el hecho de liberarnos de los cables que nos tienen atados a un lugar fijo, o cuando se necesita movilidad para trasladarse de un lugar a otro en nuestra área de trabajo sin necesidad de estar desconectando y conectando cables.

Las desventajas de este tipo de redes aun son sus costos, aunque actualmente se están reduciendo bastante, continúan siendo altos, además de la susceptibilidad de este tipo de redes a las interferencias electromagnéticas y la baja seguridad que ofrecen. A lo anterior se agrega que sus velocidades de trabajo continúan siendo menores que las que utilizan cableado.

Entre los medios no guiados se encuentran:

- Ondas de radio.
- Microondas.
- Infrarrojos.
- Ondas de luz.

- **Ondas de radio.**

Debido a que en algunos entornos el tendido de cables puede resultar muy difícil o muy frecuente debido a los cambios constantes de lugar de trabajo del personal. Se requiere utilizar redes inalámbricas que funcionan a base de tecnología de radio u ondas de radio. Las ondas de radio pueden ser omnidireccionales por lo que se propagan en todas direcciones.
Las principales técnicas utilizadas transmiten en los espectros de UHF (Ultra High Frequency, 300 Mhz-3GHz).
Las redes que operan en el espectro de UHF utilizan la banda de los 902-928 Mhz, esta banda también es usada por los teléfonos móviles o inalámbricos. Operan con una cobertura de unos pocos cientos de metros y pueden ser capaces de recorrer grandes distancias atravesando edificios y pueden obtenerse velocidades de hasta 2 Mbps.
Su gran problema son las interferencias entre usuarios.

- **Microondas.**

También se pueden utilizar redes inalámbricas que funcionan a base de tecnología de microondas. Las principales técnicas utilizadas transmiten en la banda de SHF (Super High Frequency, de 3-30 Ghz).
Las redes que operan con microondas utilizan la banda de 8 Ghz.
Estas ondas viajan en línea recta por lo que el emisor y receptor deben estar alineados. Tienen dificultades para atravesar edificios.
Se pueden alcanzar velocidades de 10-15 Mbps y distancias del orden de 100 m.
También pueden ser una forma económica de comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles ya que por la curvatura de la tierra la distancia entre dos repetidores no debe exceder de unos 80 Km de distancia.

- **Infrarrojos.**

Los haces infrarrojos son ondas direccionales incapaces de atravesar objetos sólidos como las paredes por lo que son útiles para transmisión a corta distancia.
Las redes que usan la tecnología de haces infrarrojos exigen una visión libre y sin obstáculos dada su propagación en línea recta. Cubren velocidades de 4-10 Mbps, la máxima cobertura es de tan solo unas pocas decenas de metros.

- **Ondas de luz.**

La tecnología de ondas de luz hace uso de emisiones de rayo láser para realizar la transmisión de información. Las ondas láser son unidireccionales.
Se pueden usar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

2.5.3.2 Velocidades de transmisión

La velocidad de transmisión y en consecuencia el ancho de banda requerido por las aplicaciones se ha incrementado notablemente ha medida que han ido apareciendo aplicaciones más complejas, en la Fig. 2.5.3.2.1 se observa algunos ejemplos de la evolución en el tiempo de las necesidades de ancho de banda

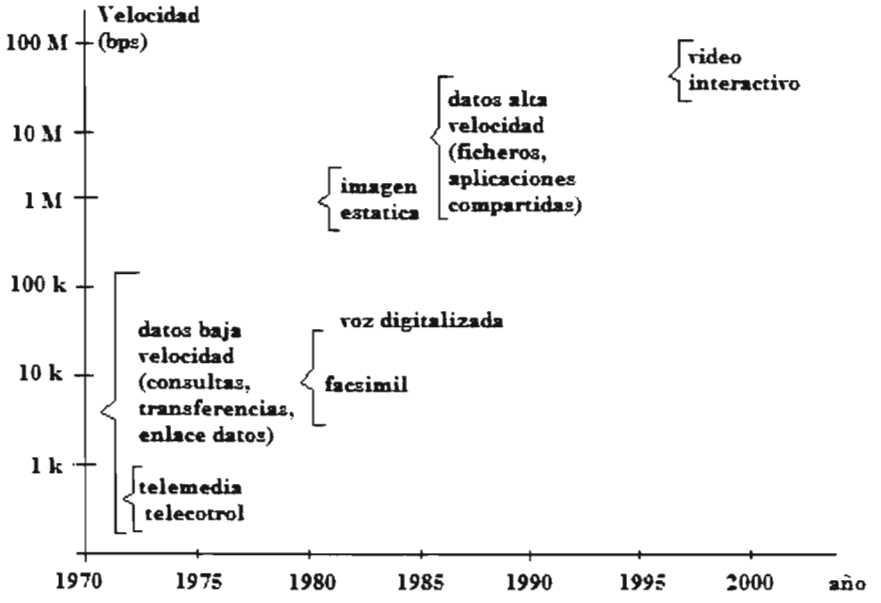


Fig. 2.5.3.2.1 Evolución de las necesidades de ancho de banda.

Las velocidades de transmisión en las redes de área local son elevadas, comparadas con las velocidades de las redes WAN, normalmente cubren el rango desde 1 Mbps hasta 100 Mbps, con la tendencia a cubrir velocidades más altas.
Existen variaos elementos que determinan la velocidad de transmisión de una red como son:

- El cable utilizado para la conexión.
- El ancho de banda permitido por el cable.
- La longitud del cable.

Otros factores determinaran el rendimiento de la red como:

- Las tarjetas de red.
- El tamaño del bus de datos de las maquinas.
- La cantidad de retransmisiones que se pueden hacer.

La tabla 2.5.3.2.1 resume las velocidades de transmisión de las redes por tipo de protocolo utilizado.

Protocolo	Cable	Velocidad	Topología
Ethernet	Par trenzado, coaxial, F.O.	10 Mbps	Bus, Estrella, Árbol
Fast Ethernet	Par Trenzado, Fibra Óptica	100 Mbps	Estrella
Gigabit Ethernet	Par Trenzado	1 Gbps	Estrella
Local Talk	Par trenzado	.23 Mbps	Bus o estrella
Token Ring	Par trenzado	4-16 Mbps	Star Wired Ring
FDDI	Fibra Óptica	100 Mbps	Anillo dual

Tecnología	Velocidad	Frecuencia	Codificación
Token ring	4 Mbps	4 Mhz	Manchester
Ethernet	10 Mbps	10 Mhz	Manchester
Token ring	16 Mbps	16 Mhz	Machester
TP-PMD	100 Mbps	62.5 Mhz 31,25 Mhz	NRZI+4B5B MLT-3+4B5B
1000BaseTX	1000 Mbps	125 Mhz	PAM-5

Tabla 2.5.3.2.1 Resumen de velocidades por protocolos

Ethernet es la tecnología predominante en las redes LAN, por eso la tabla 2.5.3.2.2 nos muestra las velocidades de transmisión en los medios de transmisión más usuales en una red LAN tipo Ethernet.

Medio	Tasa de datos	Distancia	Estándar
10Base5-Coaxial grueso	10 Mbps	500 m	IEEE802.3
10Base2-Coaxial delgado	10 Mbps	185 m	IEEE802.3
10BaseT-UTP	10 Mbps	100 m	IEEE802.3
10BaseF-Fibra Óptica	10 y 100 Mbps	2 Km	IEEE802.3
100BaseT4-UTP-Cat 3 modificado	100 Mbps	100 m	IEEE802.3u
100BaseTX-UTP-Cat 5	100 Mbps	100 m	IEEE802.3u
100BaseFX_Fibra Óptica	100 Mbps	100 m	IEEE802.3u
1000BaseT-UTP	1000 Mbps	100 m	IEEE802.3z

Tabla 2.5.3.2.2 Velocidades de transmisión en redes tipo Ethernet y Fast Ethernet

Las LAN tradicionales operan a velocidades que van de los 10 Mbps a los 100 Mbps. En la actualidad las redes LAN ya se están implementando a velocidades del orden de los Gbps.

2.5.4 Protocolos de la capa de enlace de datos

Un protocolo es un conjunto de normas y regulaciones que gobiernan la transmisión y recepción de datos, el cual rige el formato y la sincronización del intercambio de mensajes en una red de comunicaciones. En el área de redes el protocolo reúne las normas que rigen la comunicación entre computadoras en la red. Estas normas a la vez especifican que tipo de cable se utiliza, la topología de la red, que velocidad tendrán las comunicaciones y en que forma se accesara al canal de transmisión.
El protocolo va a permitir iniciar, mantener y terminar un dialogo entre elementos del sistema, regulando en que momento deberán generarse e interpretarse los elementos orientados al control de errores y la forma de recuperar los datos recibidos erróneamente, asimismo el protocolo sabrá la forma de identificar el camino que se utiliza para el intercambio de información y la identificación del tipo de mensaje.
De esta forma el protocolo define la forma en que se comunican los equipos DTE´s entre sí y los dispositivos de comunicaciones.
Durante la comunicación entre dos estaciones se tiene un control del enlace de datos que permite mantener el control del flujo de los datos. Todo el tráfico en el enlace es controlado por el protocolo de enlace (DLC). Por ejemplo si un enlace de comunicación tiene varios usuarios accesandolo, el DLC es responsable de que los datos sean transportados libres de errores para el usuario de la estación receptora en el canal. Los controles de enlace de datos siguen una secuencia de pasos bien ordenados en la administración de los canales de comunicaciones:
- Establecimiento de enlace. Una vez que el DCE tiene una conexión física con el DCE remoto, el DLC (residente usualmente en el DTE) realiza un intercambio de códigos y señales entre los terminales, previo al establecimiento de la comunicación conocido como handshaking (saludo) con el DLC lógico remoto para asegurar que ambos sistemas están listos para el intercambio de datos entre usuarios.
- Transferencia de información. Es el intercambio de datos de usuario de un lado a otro en el enlace entre dos maquinas. EL DLC verifica los datos por si existe un error de transmisión y envía un acuse de recibo de regreso a la maquina transmisora. Si en el evento es detectado un error, el receptor hace una solicitud al transmisor para retransmitir el dato.
- Terminación de enlace. Es cuando el DLC abandona el control del enlace lo que significa que más datos no pueden ser transferidos. Típicamente un DLC mantiene un enlace tan largo como el usuario disponga del envío de datos a la otra estación.
Las primeras dos capas del modelo de referencia OSI, las capas física y de enlace de datos juegan un papel muy importante en el establecimiento de las comunicaciones en una red LAN estas capas se definen en el proyecto 802. El proyecto 802 ha generado una serie de estándares para comunicaciones LAN que forman un subconjunto del modelo OSI, Fig. 2.5.4.1.

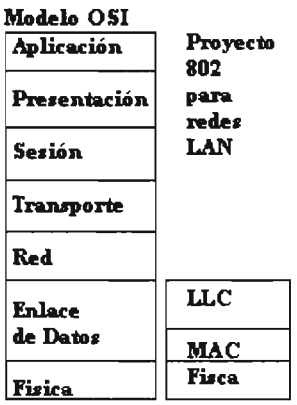


Fig. 2.5.4.1 Estándares del proyecto 802 como subconjunto del modelo OSI

La capa física de los diferentes estándares del proyecto 802 corresponde a la capa física del modelo OSI.
El proyecto 802 divide la capa de enlace de datos del modelo OSI en dos subcapas:

- La subcapa de control de acceso al medio MAC (Médium Access Control).
- La subcapa de control de enlace lógico LLC (Logical Link Control).

La razón de esta división es con el fin de que subfunciones comunes del control de enlace puedan aplicarse a todas las LAN, en tanto que las técnicas de control de acceso al medio puedan ser diferentes.

- **La subcapa de control de acceso al medio (MAC)**

En cualquier red de difusión como es el caso de las redes LAN, es bien importante determinar quien puede usar el canal cuando hay competencia por él. Los canales de difusión son conocidos como canales multiacceso o canales de acceso aleatorio. Los protocolos usados para controlar el acceso al medio pertenecen a la subcapa MAC, las funciones de la subcapa MAC son:

- Administración de acceso al medio. Esta función checa las reglas o procedimientos utilizados por los dispositivos de red para controlar el acceso al medio.
- Entramado. Se agregan encabezados de bits al inicio y al final de la trama. para indicar el inicio y final de un paquete de datos, para sincronizar al transmisor con el receptor, para el enrutamiento del paquete y para proporcionar detección de errores.
- Direccionamiento. Determinación de las direcciones de red apropiadas para identificar los dispositivos involucrados en el envío y recepción de mensajes.
- Detección de errores. Para verificar que el paquete ha sido enviado y recibido correctamente.

Para poder dar acceso al medio de transmisión en las redes de difusión se desarrollaron protocolos para permitir el acceso múltiple requerido por todas las computadoras que utilizan un medio de transmisión compartido.

El primer protocolo de acceso múltiple fue el ALOHA, el cual, en su tiempo resulto un método novedoso y elegante para resolver el problema de reparto de canal, pero este protocolo no estaba tan enfocado a redes LAN además su eficiencia no era tan buena.
En las redes LAN es posible que las estaciones detecten lo que están haciendo las demás estaciones y adapten su comportamiento con base en ello. Gracias a este comportamiento de las computadoras en una red LAN se desarrollaron los protocolos en los que las estaciones detectan una portadora (una transmisión) y actúan de acuerdo con ello, estos protocolos son conocidos como Protocolos con Detección de Portadora.

- Protocolo CSMA persistente.

El protocolo de acceso múltiple con detección de portadora CSMA (Carrier Sense Múltiple Access) persistente funciona de la siguiente forma:

1. Cuando un equipo tiene datos para transmitir primero escucha el canal para determinar si otras computadoras esta transmitiendo en ese momento.
2. Si el canal esta ocupado la computadora espera hasta que se desocupa.
3. Cuando la computadora detecta el canal en reposo, es decir sabe que esta desocupado transmite información.
4. Si ocurre una colisión, la computadora espera una cantidad aleatoria de tiempo y comienza de nuevo.

El protocolo se llama persistente por que la estación transmite con una probabilidad de 1 cuando encuentra en reposo el canal.
El retardo de la transmisión es clave para el desempeño de este protocolo ya que aunque el retardo sea cero pueden haber colisiones si coincide que dos computadoras están listas para transmitir cuando lo esta haciendo una tercera en ese momento, cuando la tercera en juego termina las dos computadoras comenzaran a transmitir ya que las dos vieron al mismo tiempo desocupado el canal, lo cual provocara una colisión, la posibilidad de colisiones aumenta con el incremento del retardo.

- Protocolo CSMA no persistente.

El protocolo de acceso múltiple con detección de portadora no persistente funciona de la siguiente forma:

1. Antes de realizar su transmisión una computadora detecta el canal, si nadie más esta transmitiendo la computadora comienza a hacerlo.
2. Si el canal ya esta en uso la computadora no observa continuamente el canal para no tomarlo inmediatamente que se desocupe de la transmisión previa como ocurre con el protocolo persistente. En cambio espera un periodo de tiempo aleatorio y repite el algoritmo. Esto conducirá a una mejor utilización del canal pero a mayores retardos que el CSMA persistente.

- **La subcapa de control de enlace lógico LLC**

La subcapa de control de enlace lógico LLC (Logical Link Control) proporciona servicios a la capa de red. Esa subcapa especifica mecanismos para direccionar computadoras a través del medio de transmisión y controlar el intercambio de datos entre dos dispositivos, se encarga también de establecer, mantener y terminar conexiones entre computadoras.
Los servicios que proporciona a la capa de red son:

1. Servicios sin acuse de recibo y sin conexión. Trafico en tiempo real: voz, redes LAN.

2. Servicio con acuse de recibo y sin conexión. Para canales inestables como sistemas inalámbricos.
3. Servicios con acuse de recibo orientado a conexión.

Los protocolos de capa de enlace más comunes son[1]:

- Ethernet
- LocalTalk
- Token Ring
- FDDI

Ethernet

Es el protocolo más común para las redes de área local actualmente, define el modo de acceso múltiple con detección de colisiones o más conocido como CSMA/CD. Este protocolo permite la conexión de terminales en bus, estrella o árbol.

Token Ring

El protocolo Token Ring popularizado por IBM tenía como método de acceso el traspaso de testigo (token passing). En una red Token Ring las estaciones se conectan formando un anillo. Un testigo (token) electrónico pasa de una estación a otra. Cuando se recibe el testigo sé esta en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre una topología de estrella cableada con par trenzado o fibra óptica. Transmiten a 4 o 16 Mbps.

FDDI

El protocolo de red FDDI (Fiber Distributed Data Interface) es muy usado para conectar dos o más redes locales que distan grandes distancias. El método de acceso al medio usado por FDDI se basa en el paso de testigo. Este tipo de protocolo utiliza una topología de anillo dual. La transmisión se realiza en uno de los anillos pero si existiera una falla en la transmisión el sistema puede utilizar una parte del segundo anillo para cerrar el anillo de transmisión. Los anillos son implementados con fibra óptica.

[1] Estos protocolos se veran con un poco de detalle en el tema 2.5.5 Estandares IEEE

2.5.5 Estándares IEEE802

El estándar para redes locales creado por el IEEE, se denomina proyecto 802. El proyecto 802 toma en cuenta las demandas que plantean los diferentes medios y las topologías empleadas en las redes locales. La tarea del IEEE 802 es la de especificar los medios mediante los cuales los dispositivos pueden comunicarse a través de una red local. De la definición del trabajo del IEEE se obtuvieron varias conclusiones una de ellas es la que dice que la tarea de comunicación a través de una red local es compleja y por lo tanto se necesita dividir en subtareas más manejables, esta conclusión se refleja en el modelo de referencia básico para redes locales mostrada en la Fig. 2.5.5.1.

Fig. 2.5.5.1 Arquitectura OSI contra arquitectura IEEE.

Los estándares IEEE 802 incluyen las normas y reglas de operación de las redes de datos y su tecnología relacionada tales como CSMA/CD, token bus y token ring. Estos estándares cubren los siguientes tópicos de las redes LAN:

- Nivel físico, relacionado con la naturaleza del medio de transmisión y con los detalles de los dispositivos de conexión y señalización eléctrica.
- Nivel de enlace que en el caso de las redes de área local se divide en dos subniveles:
  - Control de enlace lógico LLC (Logical Link Control).
  - Control de acceso al medio MAC (Medium Access Control).
- Los diferentes estándares difieren en la capa física y en la subcapa MAC pero son compatibles en la subcapa de enlace de datos.
- Los estándares IEEE 802 han sido adoptados por la ANSI y por la ISO (en la ISO se conocen como 8802).
- Los estándares 802.3, 802.4 y 802.5 describen los tres estándares para LAN CSMA/CD, Token Bus y Token Ring, respectivamente.
- Cada estándar cubre la capa física y el protocolo de la subcapa MAC.

La división del nivel de enlace es un rasgo muy particular de este estándar y refleja una de las características de la situación de las normas de las redes de área local: no existe un método de acceso al medio con un carácter suficientemente universal que pueda ser adoptado como norma única. Por otra parte permite una adaptación a las nuevas tecnologías.

Las normas del proyecto 802 creado por el IEEE para estandarizar las redes de área local se muestran en la tabla 2.5.5.1:

Estándar IEEE	Especificación
802.1	Definición de las primitivas de interfaz Normalización de interfaces de nivel superior: Niveles de aplicación, transporte y red. Puentes y gestión
802.2	Normalización para el control de enlace lógico LLC
802.3	Especificaciones Ethernet (CSMA/CD)
802.3u	Fast Ethernet: 100BaseT
802.3z	Gigabit Ethernet: 1000BaseT
802.4	Especificaciones Paso de Testigo en bus (Token Bus o Token Passing)
802.5	Especificaciones paso de testigo en anillo (Token Ring)
802.6	Especificaciones de una MAN (DQDB)
802.7	Recomendaciones para una LAN de banda ancha
802.8 y 8a	Comités de red LAN con fibra óptica
802.9	Ethernet en modo Isocrónico. Estandar para la integración de voz y datos en las redes locales
802.10	Comité de seguridad y encriptación en la LAN
802.11	Redes LAN Inalámbricas
802.12	100VY-AvyLAN

Tabla 2.5.5.1 Tabla de estándares IEEE 802

La Fig. 2.5.5.2 representa los estándares más significativos en redes de área local.

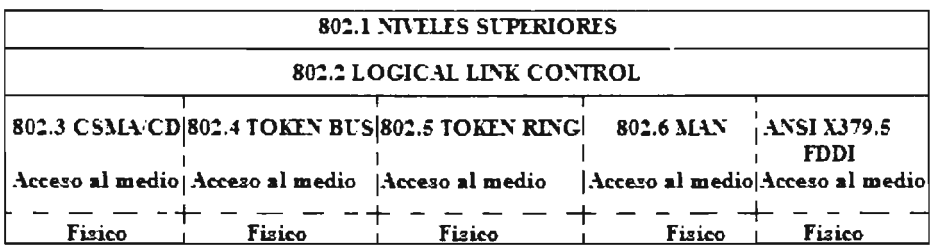


Fig. 2.5.5.2 Estándares IEEE

En el inicio del proyecto prevalecía y sigue prevaleciendo el método de acceso por contienda CSMA/CD, así como existen otros métodos de acceso en función de nuevas demandas. Con objeto de mantener los servicios proporcionados a los niveles superiores con independencia del MAC, el IEEE adopto el subnivel de control de enlace lógico, LLC, cuya estructura de trama se basa en la del protocolo HDLC.

- **Estándar IEEE 802.1**
  - El estándar 802.1 es una introducción al grupo de estándares y define las primitivas de la interfaz. También es responsable de estándares de administración de LAN.
  - El estándar 802.1 describe la parte superior de la subcapa de enlace de datos que usa el protocolo de control de enlace lógico LLC (Logical Link Control).

En la parte de normalización de la interfaz con niveles superiores es el encargado de los temas relacionados con la arquitectura de red, interconexión de redes y los aspectos relativos a la administración de la red y sus elementos.
Adicionalmente el subcomité IEEE 802.1 elabora documentos relativos a la arquitectura de red, interoperación y gestión de red.

- **Estándar IEEE 802.2**

El estándar 802.2 describe los servicios, características y protocolos del subnivel LLC (Logical Link Control), este subnivel es el nivel superior del nivel de enlace de la torre de niveles para redes de área local y es común para los diferentes métodos de acceso al medio.
Su principal función esta relacionada con la transmisión de tramas de datos entre dos estaciones sin la utilización de nodos intermedios. Algunas funciones de este subnivel son:
- Debe soportar la función multidestino.
- Algunos detalles del acceso al enlace son cubiertos por el nivel de control de acceso al medio.
- Debe proporcionar algunas de las funciones del nivel de red.

En la Fig. 2.5.5.3 se observan los requerimientos del subnivel de enlace con dos estaciones o sistemas comunicados a través de la red de área local.

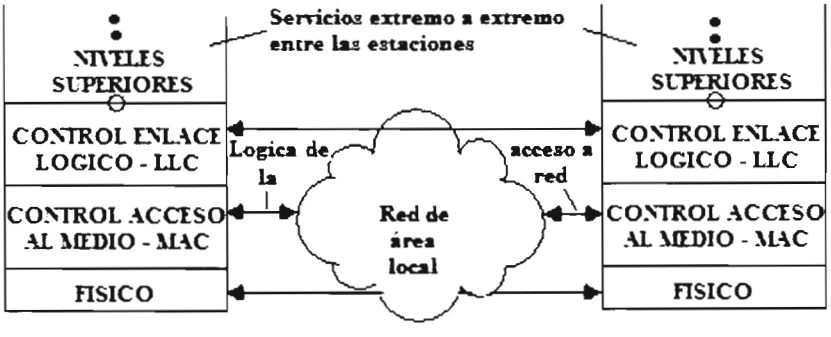


Fig. 2.5.5.3 Arquitectura de comunicación en una red LAN

Los niveles superiores (transporte hacia arriba) proporcionan un servicio extremo a extremo entre las estaciones. Por debajo del subnivel LLC el subnivel de control de acceso al medio MAC suministra la lógica necesaria en la obtención del acceso a la red para la transmisión y recepción de tramas.
El nivel LLC debe realizar las funciones asociadas al nivel de enlace:

- Control de errores extremo a extremo. El nivel de enlace debe garantizar una transmisión libre de errores a través de la red.
- Control de flujo extremo a extremo.
- Control de secuencia. Las tramas son entregadas por la red en el mismo orden en que fueron enviadas.

Como no existen nodos intermedios la red local no requiere un nivel de red independiente, así las funciones del nivel 3 se incorporan al nivel 2:

- Servicio no orientado a conexión (datagrama).
- Servicio orientado a conexión (circuito virtual).
- Multiplexación. Como la estación se conecta a la red mediante un único enlace físico, debería ser posible proporcionar transferencia de información con múltiples puntos finales en el enlace.

No habiendo necesidad de encaminamiento las tres funciones anteriores se proporcionan de manera sencilla. El servicio no orientado a conexión solamente requiere los campos de dirección de emisor y destino. La estación emisora debe indicar la dirección de destino para que el envío de la trama se realice correctamente. La dirección de emisor se indica para que el receptor sepa de donde vino la trama. Las funciones de circuito virtual y multiplexación pueden ser soportadas con el concepto de punto de acceso al servicio (SAP).
Por ultimo otra función del nivel de enlace es:

- Difusión (Mullticast, Broadcast). El nivel de enlace debería proporcionar un servicio de envío de mensajes a múltiples estaciones o a todas.

En forma general la norma 802.2 describe las especificaciones de la interfaz de servicio del subnivel LLC con:

- Nivel de red (N3): define una descripción de los diversos servicios que el subnivel LLC ofrece a dicho nivel.
- Subnivel MAC. Define una descripción de los servicios que el subnivel LLC requiere del subnivel MAC.
- Función de gestión del subnivel LLC: Proporciona una descripción de los servicios de administración proporcionados al subnivel LLC por la función de gestión del subnivel LLC.

El estándar IEEE 802.2 especifica tres tipos de servicio proporcionados por el LLC a los usuarios a través de los puntos de acceso al servicio LLC (LSAPs):

1. Servicio no orientado a conexión sin reconocimiento (Unacknowledge connectionless service).
2. Servicio orientado a conexión (Connection mode service).
3. Servicio no orientado a conexión con reconocimiento (Acknowledge connectionless service).

Servicio no orientado a conexión sin reconocimiento. Subnivel LLC.
Es un servicio que simplemente permite el envío y recepción de datos. El suministrador del servicio no garantiza que los datos vayan a llegar al destino, ni informa al emisor de los posibles fallos en la comunicación, así como no se hace responsable de que los datos lleguen en el orden en que fueron enviados. Este tipo de operación es útil cuando los niveles superiores proporcionan un servicio de recuperación y control de secuencia tal que no requieren ser referenciados por el nivel de enlace, asimismo se usa en aplicaciones en las que no es esencial garantizar el envío de cada unidad de datos en el nivel de enlace.
Este servicio emplea dos primitivas:
DL-UNITDATA.request(dirección propia, dirección destino, datos, prioridad)
DL-UNITDATA.indication(dirección propia, dirección destino datos, prioridad)
La primitiva request es emitida por el nivel de red al LLC, Fig. 2.5.5.4, para solicitar la transferencia de una unidad de datos de servicio. Los parámetros de dirección corresponden a la combinación de las direcciones SAP, LLC y MAC. La dirección destino puede especificar una dirección individual o colectiva. La prioridad se usa para darle prioridad a la trasferencia, la cual se pasa al nivel MAC para que se haga cargo de implementar el mecanismo de prioridad, mecanismo ya incluido en los protocolos de paso de testigo en bus, anillo y FDDI, en CSMA/CD no esta incluido.
La primitiva indication se emite desde el LLC al nivel de red para indicar la llegada de una unidad de datos.

Fig. 2.5.5.4 Diagrama de la relación de primitivas de un servicio no orientado a conexión sin reconocimiento.

Servicio orientado a conexión. Subnivel LLC.

En este servicio existe un acuerdo entre los dos usuarios LLC para el intercambio de información en tres fases:

a. Establecimiento de la conexión.
b. Transferencia de datos.
c. Finalización de la conexión.

a. Establecimiento de la conexión.

Uno de los usuarios solicita una conexión a otro usuario, Fig. 2.5.5.5.

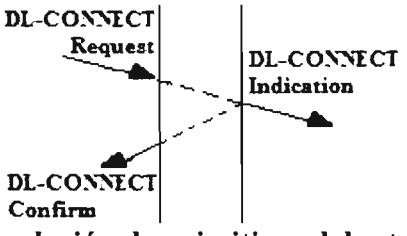


Fig. 2.5.5.5. Diagrama de la relación de primitivas del establecimiento de conexión en un servicio orientado a conexión

La conexión lógica se establece en el caso de que el LLC sea capaz de proporcionar el servicio solicitado y el usuario destino este preparado para el intercambio de datos. Mediante esta conexión el LLC es capaz de controlar las unidades de datos transmitidas y recibidas. Se emplean tres primitivas:

DL-CONNECT.request(dirección propia, dirección destino, prioridad)
DL-CONNECT.indication(dirección propia, dirección destino, prioridad)
DL-CONNECT.confirm(dirección propia, dirección destino, prioridad)

b. Transferencia de datos.

Una vez establecida la conexión entre los dos usuarios LLC definidos por sus SAPs correspondientes se produce la transferencia de información. En esta fase el LLC garantiza que todas las unidades de datos se transmiten y en el orden correcto, se emplean dos primitivas:

DL-DATA.request(dirección propia, dirección destino, datos)
DL-DATA.indication(dirección propia, dirección destino, datos)

Esta fase de transferencia de datos solo tiene dos primitivas ya que el usuario no tiene necesidad de confirmar los datos enviados por que el LLC garantiza su transmisión libe de errores, si existieran problemas se usan las funciones de disconnect o reset. Durante esta transferencia de datos se emplea el servicio de control de flujo para controlar la cantidad de datos que se pasan entre el nivel de red y el LLC, para esto se usan las siguientes primitivas:

DL-CONNECTION-FLOWCONTROL.request(dirección propia, dirección destino, cantidad de datos)
DL-CONNECTION-FLOWCONTROL.indication(dirección propia, dirección destino, cantidad de datos)
La cantidad de datos se define en cada <request> o <indication>. Si es cero se detiene la transmisión.
La reiniciación o reset de la transferencia provoca que todas las unidades de datos de las que no se ha recibido confirmación sean descartadas. El LLC no recupera esos datos por lo que esto es asumido por un protocolo de nivel superior. Las primitivas para la reiniciación son:
DL_RESET.request(dirección propia, dirección destino)
DL-RESET.indication(dirección propia, dirección destino, motivo)
DL_RESET.confirm(dirección propia, dirección destino)

c. Finalización de la conexión.

Esta fase es iniciada tanto por los usuarios LLC como por el propio LLC para dar fin a la conexión lógica y desechar las unidades de datos pendientes mediante el uso de las primitivas:
DL_DISCONNECT.request(dirección propia, dirección destino)
DL_DISCONNECT.indication(dirección propia, dirección destino, motivo)
El parámetro motivo indica la razón de la desconexión, esta fase se muestra en la Fig. 2.5.5.6

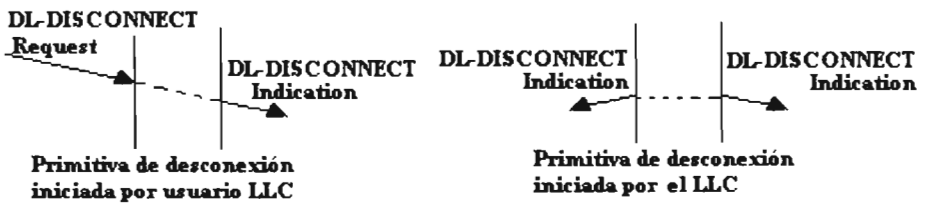


Fig. 2.5.5.6 Primitivas de desconexión iniciadas por usuarios y por el LLC

Servicio no orientado a conexión con reconocimiento. Subnivel LLC.

En este servicio no se establece una conexión lógica previa, pero si proporciona un reconocimiento inmediato de las unidades de datos enviadas, de esta manera solo se transmite una unidad de datos a la vez, esperándose a recibir la correspondiente confirmación antes de transmitir la siguiente. Este servicio a su vez tiene dos servicios:

a. DL-DATA-ACK
b. DL-REPLY

a. DL-DATA-ACK.

En este servicio la entrega no esta garantizada, los datos se envían desde el LLC a la vez que se solicita su reconocimiento, mediante las siguientes primitivas:
DL-DATA-ACK.request(dirección propia, dirección destino, datos, prioridad, clase de servicio)
DL-DATA-ACK.indication(dirección propia, dirección destino, datos, prioridad, clase de servicio)

DL-DATA-ACK-STATUS.indication(dirección propia, dirección destino, prioridad, clase de servicio, estado)
Las primitivas <request> <indication> se emiten por el nivel de red al LLC para solicitar la transferencia de datos de servicio. Los parámetros dirección corresponden a la combinación de direcciones SAP, LLC y MAC. Además indican una solicitud de reconocimiento. La clase de servicio indica si el nivel MAC va a participar en el reconocimiento de la transmisión de datos.
La primitiva STATUS.indication proporciona el reconocimiento al usuario emisor. El parámetro estado indica si los parámetros fueron recibidos correctamente o no. Estas transferencias se muestran en la Fig. 2.5.5.7

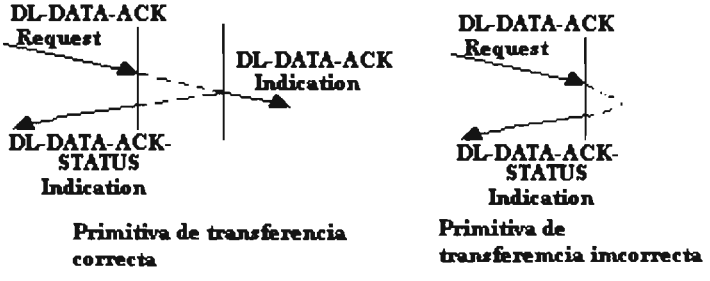


Fig. 2.5.5.7 Diagrama de las primitivas de transferencia correcta e incorrecta. DATA-ACK.

b. DL-REPLY.

Este servicio se utiliza para consulta o poleo (polling) con garantía de respuesta, para solicitar a otro usuario unidades de datos previamente preparados o intercambiar unidades de datos con otro usuario. El suministrador de servicio LLC puede retener una unidad de datos y pasarla al usuario que la solicite, para esto el usuario LLC le envía los datos previamente o el usuario puede consultar directamente al usuario remoto para pedirle los datos como muestran la Fig. 2.5.5.8

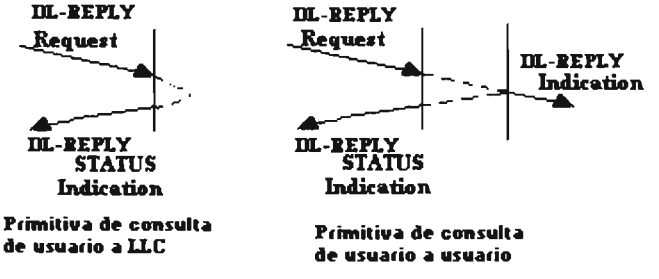


Fig. 2.5.5.8 Diagrama de primitivas del servicio de consulta.

Las primitivas de este servicio son:
DL-REPLY.request(dirección propia, dirección destino, datos, prioridad, clase de servicio)
DL-REPLY.indication(dirección propia, dirección destino, datos, prioridad, clase de servicio)
DL-REPLY-STATUS.indication(dirección propia, dirección destino, datos, prioridad, clase de servicio, estado)
DL-REPLY-UPDATE.request(dirección propia, estado)
DL-REPLY-UPDATE.indication(dirección propia, estado)
Estas primitivas proporcionan servicio de intercambio de datos.

Protocolo del subnivel LLC

Las principales características del protocolo LLC son:

- Utiliza el modo de operación asíncrono balanceado de HDLC para soportar el servicio LLC orientado a conexión.
- LLC utiliza la PDU de información no numerada para soportar el servicio no orientado a conexión sin reconocimiento.
- LLC implementa la múltiplexación mediante el uso de los LSPAs (Puntos de Acceso al Servicio del subnivel LLC).
- LLC utiliza dos nuevas PDUs no numeradas para soportar el servicio no orientado a conexión con reconocimiento.

Unidad de datos de protocolo LLC

El formato de la LLC PDU (Unidad de datos de protocolo) representa las direcciones de los LLC SAP (Puntos de acceso al servicio) desde o hacia las entidades del nivel de red, Fig. 2.5.5.9

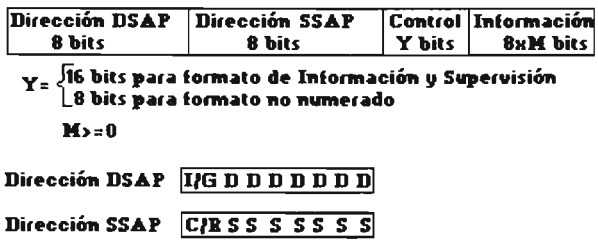


Fig. 2.5.5.9 Formato de la LLC PDU

De los dos campos de direcciones uno es el DSAP y el otro el SSAP:

- DSAP (Punto de Acceso al Servicio Destino), identifica el SAP al que va dirigido el campo de información. El bit I/G indica si la dirección destino es una dirección individual (I/G=0) o de grupo (I/G=1).
- SSAP (Punto de acceso al servicio fuente), identifica el SAP en el que el campo de información fue generado. El bit C/R indica si la LLC PDU es un mandato (C/R=0) o si es una respuesta (C/R=1)

Todos los bits D o S a 0 identifican una dirección nula, lo cual designa el LLC asociado con el MAC subyacente y no se usa para identificar ningún SAP al nivel de red.

LLC requiere las direcciones fuente y destino para identificar las dos entidades que se comunican, tanto la fuente como el destino son identificadas de manera univoca por el par (nodo, SAP).

Dependiendo de la operación por cada servicio definido se tienen tres tipos de protocolos LLC:

1. Operación tipo 1 soporta el servicio no orientado a conexión sin reconocimiento.
2. Operación tipo 2 soporta el servicio orientado a conexión
3. Operación tipo 3 soporta el servicio no orientado a conexión con reconocimiento.

Todos los protocolos LLC emplean el mismo formato de PDU. La tabla 2.5.5.2 muestra las PDUs usadas en LLC.

Nombre	Función	Descripción
Servicio no orientado a conexión sin reconocimiento		
Unumbered (U)		
UI(unnumbered information)	C	Intercambio de datos
XID (exchange identification)	C/R	Tipo de operación y tamaño de
		ventana
Test	C/R	Test
Servicio orientado a conexión		
Information (I)	C/R	Intercambio de datos
Supervisory (S)		
RR (receive ready)	C/R	Reconocimiento positivo
		preparado para recibir PDU
RNR (receive not ready	C/R	Reconocimiento positivo
		no preparado para recibir
REJ (reject)	C/R	Reconocimiento negativo
Unnumbered		
SABME (set asynchronous	C	Petición de conexión
Balance mode extended)		
DISC (disconnect)	C	Conexión terminada
UA (Unumbered	R	Comando confirmación no
Acknowledgment)		Numerada
DM (disconnect mode)	R	Rechazo de conexión
FRMR (frame reject)	R	Información de trama rechazada
Servicio no orientado a conexión con reconocimiento		
Unumbered		
AC (aknowledged	C/R	Intercambio de datos
Connectionless information)		

Tabla 2.5.5.2 Unidades de datos de protocolo LLC

Operación tipo 1

Emplea la PDU UI en la transferencia de datos. No hay reconocimiento o confirmación, ni control de errores de flujo, pero si detección y descarte de errores en el nivel MAC. La PDU XID indica el tipo de operación soportado y e tamaño de la ventana de transmisión. La PDU Test comprueba el enlace de transmisión entre dos entidades LLC. Cuando recibe una PDU Test en modo mandato (bit C/R=0) la entidad LLC receptora emite una PDU Test en modo respuesta (bit C/R=1).

Operación tipo 2

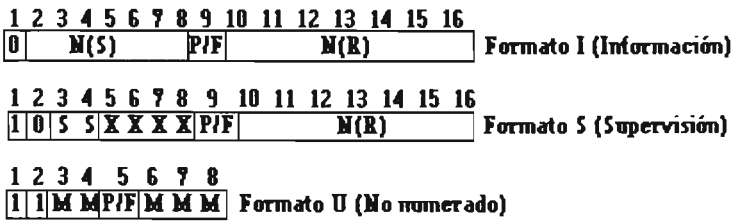
Establece una conexión lógica entre las entidades LLC previa al intercambio de información. Así la entidad LLC envía una PDU SABME a la entidad remota, si se acepta la solicitud la entidad LLC devuelve una PDU UA, de esta forma la conexión se identifica con los SAPs de los usuarios. Si se rechaza la solicitud se envía una PDU DM. Una vez establecida la conexión las PDUs I de información se emplean para el intercambio de datos. La PDU I incluye los números de secuencia de emisión y recepción para el control de

secuencia y flujo. La PDU S de supervisión se utiliza para el control de errores y de flujo. Para solicitar el reset de una determinada conexión se emplea la PDU SABME con las direcciones apropiadas DSAP y SSAP. El usuario LLC remoto acepta la reiniciación respondiendo con una PDU UA o la rechaza con una PDU DM. Cuando se produce el reset ambas entidades LLC inicializan a cero sus números de secuencia de emisión y recepción. Para finalizar la conexión las entidades LLC envían la PDU DISC.

Operación tipo 3

En este tipo de operación los datos enviados a través de una PDU AC en modo mandato deben recibir la confirmación mediante otra PDU AC en modo respuesta. Para el control de posibles pérdidas de PDUs se utiliza un número de secuencia de 1 bit. El emisor alterna en sus PDUs los números de secuencia 0 y 1, respondiendo el receptor en sus PDUs con el número de secuencia opuesto al que se recibió.

El campo de control se forma de uno o dos octetos usados par designar mandatos y funciones de respuesta y podrán contener números de secuencia si es necesario, Fig. 2.5.5.10.



Donde:
N(S) es el número de secuencia de la LLC PDU enviada
N(R) es el número de secuencia de la última PDU recibida correctamente
S son los bits cuyo valor indica el tipo de función de supervisión de la LLC PDU con formato S
X bits reservados que se ponen a cero
M bits que determinan la función no numerada ejercida por una LLC PDU con formato U
P/F bit polling/final

Fig. 2.5.5.10 Formato del campo de control LLC PDU

En el formato del campo de control podemos ver que se tienen tres tipos de tramas para LLC: transferencia e información, supervisión y no numerado., el uso de cada trama depende del tipo de operación empleado.

El formato PDU de transferencia de información se emplea en transferencias de información numerada en operaciones de tipo 2. N(S) y N(R) son números de secuencia de tramas que soportan control de error y control de flujo. La secuencia emisora enumerara sus tramas y pondrá su numero en el campo N(S). N(R) permite a la estación indicar él número de la siguiente trama que espera recibir. Estos números soportan control de flujo mediante el procedimiento de ventana deslizante.

El formato PDU de supervisión S se utiliza para realizar funciones de control y supervisión del enlace de datos en operaciones tipo 2. La función es determinada por los bits S del campo de control:

SS: 00 Receiver Ready (RR)
01 Reject (REJ)
10 Receiver Not Ready (RNR)

RR reconoce la última trama recibida indicando en N(R) la siguiente trama esperada. RNR reconoce una trama pero solicita a la estación emisora la suspensión de la transmisión. Cuando la estación receptora esta de nuevo preparada envía una trama RR. REJ indica que la trama con numero N(R) es rechazada y que esta así como las siguientes tramas deben ser enviadas de nuevo.
El formato U no numerado se emplea en operaciones del tipo 1 y 2, dependiendo de la función definida por los valores de los bits M del campo de control:

- SABME se utiliza por una entidad LLC para solicitar una conexión con otra entidad LLC.
- DISC se emplea para terminar una conexión lógica, la estación emisora esta anunciando que va a suspender las operaciones.
- UA se utiliza para confirmar los mandatos SABME y DISC.
- DM indica en respuesta a una trama, que el LLC de la estación esta lógicamente desconectado.
- FRMR indica que se ha recibido una trama inapropiada al protocolo.
- AC se utiliza para información de reconocimiento en operación de tipo 3.

El campo de información se compone de un número entero de octetos, incluido ninguno. El valor máximo de M dependerá de la metodología de control de acceso al medio utilizado.

Resumen IEEE802.2
El estándar IEEE 802.2 define los servicios, protocolos y características del subnivel de enlace lógico de datos LLC, el cual constituye el nivel superior de la arquitectura de comunicaciones de las redes locales, situándose por encima de los diferentes métodos de control de acceso al medio MACs y por lo tanto siendo común a todos ellos. Su objetivo principal es proporcionar los mecanismos necesarios para el intercambio de datos entre usuarios LLC a través de la red local. Se especifican tres clases de servicio LLC en función de la confiabilidad y eficiencia necesarias: servicio no orientado a conexión, servicio orientado a conexión y servicio no orientado a conexión con reconocimiento.

- **Estándar IEEE 802.3/Ethernet**

El estándar IEEE 802.3 se deriva de la tecnología estándar de redes de área local Ethernet. Este tipo de redes son redes de transmisión por difusión, lo que significa que todas las estaciones ven todos los paquetes. Cada estación debe examinar los paquetes recibidos para determinar si la estación es un destino. Las estaciones CSMA/CD pueden detectar colisiones y determinar cuando retransmitir.
Las redes ethernet definen un método de acceso múltiple y detección de colisiones CSMA/CD y corren por una variedad de tipos de cable a 10 Mbps. Así el estándar IEEE 802.3 es una recomendación para el control de acceso al medio (MAC) mediante la técnica de acceso múltiple con detección de portadora y detección de colisión (CSMA/CD- Carrier Sense Multiple Access with Collision Detection).
La tecnología Ethernet consiste básicamente en un cable coaxial llamado ether de aproximadamente pulgada de diámetro y hasta 500 metros de longitud. Estos pueden ser extendidos por medio de los dispositivos repetidores que duplican las señales eléctricas de un cable a otro. Ethernet suele usarse para referirse a todas las LANs que utilizan la técnica de acceso al medio CSMA/CD (Carrrier Sense Múltiple Access with Collision Detection) que cumplen con las especificaciones Ethernet e IEEE 802.3 operando en banda base sobre el cable coaxial, siendo esta la especificación original y posteriormente se desarrollaron

variaciones para CSMA/CD banda base sobre cable coaxial fino y par trenzado, así como banda ancha y operación a 100 Mbps. Ethernet esta bien adaptada a las aplicaciones en que el soporte de comunicaciones local a menudo tiene que procesar un elevado trafico con puntas elevadas de intercambio de datos.

El funcionamiento de la red LAN ethernet /IEEE802.3 explica a continuación:

La técnica de acceso al medio del estándar IEEE 802.3 es CSMA/CD, en este modo de operación las estaciones en una LAN CSMA/CD pueden acceder a la red en cualquier momento y antes de enviar los datos las estaciones CSMA/CD escuchan la red para ver si es operativa, es decir si esta transmitiendo (detección de portadora). Si lo esta, la estación que desea transmitir espera. Si la red no esta en uso, la estación transmite sus datos. Se produce una colisión cuando dos estaciones que escuchan la red no oyen nada y/o transmiten simultáneamente. En este caso ambas transmisiones quedan descartadas ya que se interfieren entre ellas y las estaciones deben transmitir en otro momento.

Ya que solo una estación puede transmitir en un momento dado o espacio de tiempo dado, se usa un mecanismo de control para determinar el procedimiento a seguir por la estación cuando encuentra el medio ocupado u ocurre una colisión:

1. Si el medio esta libre se realiza la transmisión, si no se sigue el paso 2.
2. Si el medio esta ocupado continua escuchando hasta que se libere para transmitir inmediatamente.
3. Si existe una colisión en la transmisión, se transmite una señal de colisión o jamming para asegurar que todas las estaciones han reconocido la colisión y cesen la transmisión.
4. Después de transmitir la señal de colisión se realiza una pausa de tiempo aleatorio y se intenta transmitir nuevamente comenzado el procedimiento en el paso 1.

El estándar IEEE 802.3 exige que las tramas a utilizar deben ser lo suficientemente grandes para permitir la detección de la colisión antes de la finalización de la transmisión. El estándar especifica que el tamaño sea de 512 bits o 64 octetos equivalentes a 51.2 microsegundos.

Para evitar que dos estaciones involucradas en una colisión vuelvan a retransmitir al mismo tiempo y se vuelvan a colisionar, cada estación retrasa su retransmisión cierto tiempo determinado por una distribución aleatoria, para esto se usa un algoritmo conocido como truncated binary exponential backoff para determinar cuando deben retransmitir las estaciones que han colisionado. El mecanismo de backoff determina el retardo que debe esperar la estación antes de retransmitir, el cual es igual a un numero entero de tiempos de ranuras o time slot (valor superior a dos veces el tiempo que tarda la señal en recorrer el medio de un extremo a otro mas el tiempo de la señal de jam del subnivel MAC). Después de un número indefinido de intentos, la entidad MAC asume la existencia de un problema y abandona la transmisión informando del error al LLC.

Ethernet e IEEE 802.3 no son idénticos, aunque son capaces de coexistir en el mismo medio. Prácticamente la única diferencia entre ethernet e IEEE802.3 es que ethernet proporciona servicios correspondientes a las capas 1 y 2 del modelo de referencia OSI. mientras que IEEE 802.3 especifica la capa (capa 1) y la parte de acceso al medio de la capa de enlace (capa 2), pero no define un protocolo de control de enlace lógico, es decir la diferencia reside en la cabecera del paquete de red.

La arquitectura IEEE802.3 comprende los siguientes niveles:

- Subnivel MAC
  - Especificaciones de servicio MAC.
  - Protocolo y unidades de datos MAC.

- Nivel físico
- Especificaciones de servicio.
- Especificaciones independientes del medio.
- Especificaciones del medio físico.

Especificaciones de servicio del subnivel MAC. Estándar IEEE802.3

Estas especificaciones definen el servicio proporcionado por el IEEE 802.3 al LLC, las cuales incluyen facilidades para la transmisión y recepción de PDU y suministran información del estado de las operaciones para recuperación de errores de niveles superiores. Las primitivas son:

- MA_DATA.request(dirección destino, m_sdu, clase de servicio solicitada por niveles superiores).

Esta primitiva la genera el subnivel LLC siempre que deba transferir datos a otras entidades del subnivel LLC.

- MA_DATA.indication(dirección destino, dirección propia, m_sdu, estado de recepción, calidad de servicio solicitada para esa transferencia).

Esta primitiva la pasa el subnivel MAC al subnivel LLC para indicarle la llegada de una trama a la entidad local del subnivel MAC.

- MA_DATA.confirm(estado de transmisión, clase de servicio proporcionada).

Protocolo del subnivel MAC. Estándar IEEE802.3

El protocolo MAC es el núcleo de la norma 802.3 que a menudo se conoce simplemente como estándar CSMA/CD. La especificación describe la estructura de trama y las interacciones que tienen lugar entre las entidades MAC. CSMA/CD define sobre la estructura del subnivel MAC el marco estructural para sistemas de comunicaciones de datos empleando procedimientos del subnivel MAC.

El formato de la trama MAC para los estándares ethernet e IEEE802.3, así como sus campos se muestran en al Fig. 2.5.5.11

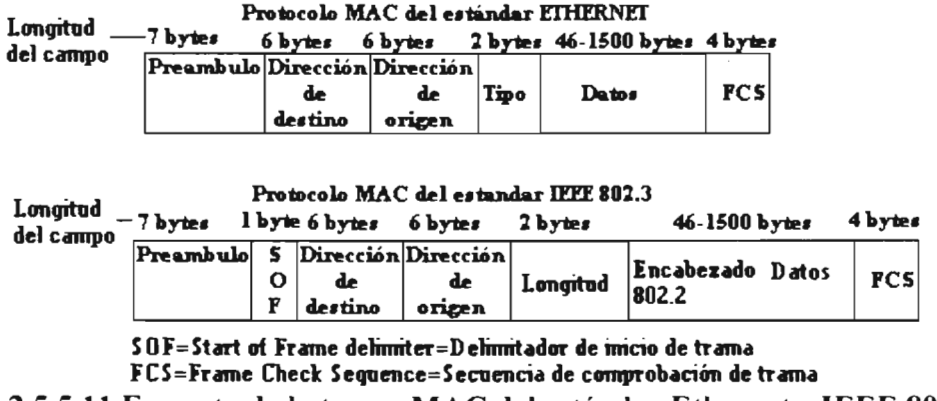


Fig. 2.5.5.11 Formato de la trama MAC del estándar Ethernet e IEEE 802.3

Como se puede observar en la Fig. 2.5.5.11 Ethernet define en su trama de que manera se introducirán los datos en la red. Indica el receptor, el emisor, donde iran los datos, donde ira el checksum, etc. En la misma Fig. 2.5.5.11 se observa la trama del estándar IEEE802.3 la trama comienza con un preámbulo, al cual le sigue la trama en si con un inicio de trama, al inicio de trama le sigue la información de las direcciones destino y origen, y a estas les

sigue el tipo de información de los datos y el checksum de la trama, sus campos son los siguientes:

- Preámbulo. En la estructura del marco 802.3 de la Fig. 2.5.5.11 cada marco comienza con un preámbulo de 7 bytes, cada uno de los cuales contiene el patrón de bits 10101010.
- Delimitador de partida. A continuación del preámbulo viene un byte de inicio de marco o de trama SOF (Start of Frame delimiter-Delimitador del inicio de trama) que contiene el patrón 10101011 para indicar el inicio del marco mismo.
- El marco tiene dos direcciones, origen (estación de la que se envía el paquete) y destino (dirección a la cual el paquete va dirigido puede ser individual o de grupo) que pueden ser de 2 o de 6 bytes, para banda base de 10 Mbps se usan 6 bytes. El bit 46 o de mayor orden de la dirección destino distingue entre direcciones locales y globales, es 0 para direcciones ordinarias y 1 para direcciones de grupo (multidifusión). La dirección de puros 1´s esta reservada para difusión o broadcast.
- El campo tipo en la trama Ethernet tiene el objeto de identificar cada uno de los protocolos particulares. Los valores del campo tipo son: Hex 0600 para el protocolo XNS de Xerox, Hex 0800 para IP, Hex 6003 para DECNET y Hex 0806 para ARP. El estándar Ethernet no necesitaba del campo de longitud por que los protocolos particulares que lo utilizaban tenían todos sus propios campos de longitud.
- El campo longitud indica cuantos bytes están presentes en el campo de datos (0-1500).
- Campo de datos (LLC Data) y relleno (Pad). El campo de datos contiene una secuencia de n octetos, aunque las tramas validas según 802.3 deben ser de al menos 46 bytes de longitud, desde la dirección destino hasta la suma de comprobación o sea debe ser ≥46 bytes. Si no se alcanza el tamaño mínimo el subnivel MAC añadirá automáticamente unos octetos (PAD) hasta obtener dicho tamaño mínimo necesario.
- Secuencia de verificación. El campo final del 802.3 es la suma de comprobación de trama FCS (Frame Check Séquence) que es el código de dispersión de 32 bits de los datos el cual usa un algoritmo de verificación de redundancia cíclica (CRC) para generar este campo de 4 octetos sobre la base del polinomio generador $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$.

En el estándar 802 el tipo esta implícitamente incluido en la cabeceras SAP del 802.2. Esta cabecera se encapsula en la trama 802.3. La cabecera 802.2, Fig. 2.5.5.12 formada por tres bytes se emplea para el control de las tramas o para el tipo de datos no orientados a conexión enviados por los antiguos protocolos DIX. Para los datos orientados a conexión se define una cabecera de 4 bytes que hace referencia principalmente a los protocolos SNA y NETBEUI. Los dos primeros bytes de la cabecera identifican el punto de acceso al servicio SAP. Los dos campos SAP se definen con los valores Hex 0404 para SNA y Hex E0E0 para NETBEUI.

DSAP	SSAP	Control
8 bits	8 bits	8/16 bits

Fig. 2.5.5.12 Formato de la cabecera IEEE802.2

Las funciones que realiza el subnivel MAC son las siguientes:

- En la transmisión de tramas. En esta parte se encapsulan los datos a transmitir (ensamblado de la trama, generación de secuencia de verificación de trama), se realiza la gestión de acceso al medio (detección de portadora, espaciamiento entre

tramas, detección y resolución de colisiones, backoff y retransmisión) y se asegura un tamaño mínimo de trama.

- Acepta solo datos del subnivel LLC y se construye una trama, los campos de la trama son puestos a partir de los que proporciona el subnivel LLC.
- Presenta una serie de bits al nivel físico para su transmisión sobre el medio.
- Detección de portadora muestreando el medio físico, se retrasa la transmisión de los bits si el medio físico esta ocupado. Después de que el ultimo bit de la trama que ocupaba el medio lo deja libre, el subnivel CSMA/CD espera un espacio interframe y se inicia la transmisión.
- Se añade la correcta verificación de trama FCS, añadiendo el código CRC a las tramas antes de transmitir.
- Retrasa la transmisión de bits durante el espacio intertramas para asegurar un mínimo espacio que proporcione un tiempo de recuperación para otros subniveles MAC CSMA/CD y para el nivel físico.
- Cuando se detecta una colisión mediante la señal de detección de colisiones que proporciona el medio físico, la transmisión no finaliza inmediatamente, esta continúa hasta que los bits que forman el mensaje jam han sido transmitidos. Estos bits del mensaje jam aseguran que la duración de la colisión es suficiente para ser detectada por todas las estaciones.
- Planifica la retransmisión después de una colisión retardando un tiempo (backoff) la transmisión hasta que se realice correctamente o hasta que se alcanza un numero máximo de reintentos.
- Se envía la secuencia jam para que todos detecten la colisión.
- Se añade el preámbulo SFC, DA, SA, campo de longitud y FCS a todas las tramas y se inserta el PAD a la trama con longitud de datos del LLC menor al valor mínimo, antes de calcular y añadir la secuencia FCS.

• En la recepción de tramas. Maneja los aspectos de desencapsulamiento de tramas (reconocimiento de dirección, validación de la secuencia de verificación de trama y su desensamblado) y de gestión de acceso al medio (determinación de los limites de la trama así como el filtrado de colisiones).

- Recibir los bits desde el nivel físico.
- Presentar tramas al subnivel LLC.
- Reconocimiento de la dirección individual o de grupo.
- Descartar o pasar la gestión de la red y todas las tramas no direccionadas a la estación receptora.
- Comprobar la FCS para las tramas recibidas. La validación de FCS es idéntica a su generación. Si los bits de la trama que llega no generan un CRC idéntico al recibido, se detecta un error y la trama es calificada como invalida.
- Quitar el preámbulo SFD, SA, DA, campo de longitud y PAD de las tramas recibidas.
- El subnivel MAC CSMA/CD reconoce el limite de la trama que llega muestreando la señal detectora de portadora que proporciona el PLS, puede haber dos errores de longitud de trama, tramas demasiado largas y longitud de trama sin un numero entero de octetos. Estas tramas se rechazan y se informan como errores.
- Para el filtrado de colisiones se descartan los fragmentos de trama que se suponen son producto de una colisión.

- Si no hay errores la trama es desensamblada y los datos del campo de datos se pasan al subnivel LLC.

Las primitivas para servicios de interacción entre niveles MAC son las siguientes:
- PLS:DATA.request (OUTPUT_UNIT)
Esta primitiva es generada por el subnivel MAC para solicitar la transmisión de un bit de datos sobre el medio físico o para detener la transmisión. El parámetro OUTPUT_UNIT representa un único bit de datos y puede tener tres valores 0, 1 o DATA_COMPLETE, este último valor indica que el subnivel AC no tiene más datos para enviar.
- PLS:DATA.confirm, (OUTPUT_STATUS)
Esta es la respuesta a la anterior primitiva. El parámetro OUTPUT_STATUS puede tener cualquiera de los dos valores siguientes:
OTPUT_NEXT que significa que el subnivel PLS esta preparado para otra petición desde el subnivel MAC.
OUTPUT_ABORT indica que el subnivel PLS no puede completar la petición recibida de envío de un bit de datos.
- PLS_DATA.indication (INPUT_UNIT)
Esta primitiva se genera para todas las entidades MAC de la red. El parámetro INPUT_UNIT puede tener cualquiera de los dos valores que representan a un bit 0 o 1.
Las primitivas para servicios de interacción entre los subniveles MAC y PLS son:
- PLS_CARRIER.indication (CARRIER_STATUS)
Transfiere el estado de la actividad en el medio físico, desde el subnivel PLS al subnivel MAC. El parámetro CARRIER_STATUS indica la presencia o no de la señal.
- PLS_SIGNAL.indication (SIGNAL_STATUS)
Transfiere el estado de la calidad de la señal del nivel físico, desde el subnivel PLS al subnivel MAC. El parámetro SIGNAL_STAUTS indica si se recibe o no la señal adecuada.

Especificaciones independientes del medio del estándar IEEE802.3.
En el estándar IEEE 802.3 la codificación de la señal se realiza mediante el código Manchester con lo que se garantizan las transiciones necesarias para realizar la sincronización aunque la velocidad en baudios se duplica. También el estándar especifica las velocidades de transmisión de 1, 10 y 100 Mbps para el par trenzado no apantallado y 10 para el coaxial.

Especificaciones dependientes del medio del estándar IEEE802.3
La norma ha definido diferentes tipos de medios de transmisión y distintas topologías para dar soluciones a diferentes clases de aplicaciones. Estos tipos son 10BASE5, 10BASE2, 10BASET, 10BROAD36, FAST ETHERNET (100BASET), Gigabit Ethernet. En estos tipos la notación indica tres parámetros el primero es la velocidad (10 y 100), el segundo es el tipo de transmisión (Banda base y banda ancha) y el tercero la longitud del segmento en centenares de metros, para (10BASET y 100BASET el tercer parámetro indica el tipo de medio utilizado que es par trenzado). La tabla 2.5.5.3 muestra las principales características de cada especificación.
Las características del nivel físico del estándar IEEE802.3 son:

- La transmisión se realiza en banda base, es decir sin modulación, por lo cual se ocupa todo el ancho de banda con cada transmisión.
- Las velocidades de transmisión estándares son 1 y 10 Mbps.
- El numero máximo de estaciones en una red de este tipo es de 1024.

- La longitud máxima por segmento de cable es de 500 metros.
- La distancia máxima permitida entre estaciones situadas en diferentes segmentos es de 2.5 Km.
- El numero máximo de estaciones por segmento es de 100.
- Se permiten hasta 4 repetidores por segmento.
- Permite la conexión de diferentes sistemas.

Parámetro	10BASE5	10BASE2	1BASE5	10BASET	10BROAD36
Medio de transmisión	Coaxial 50 ohm	Coaxial 50 ohm	UTP	UTP	Coaxial 75 ohm
Técnica de señalización	Banda base Manchester	Banda base Manchester	Banda Base Manchester	Banda Base Manchester	Banda ancha (DPSK)
Velocidad	10 Mbps	10 Mbps	1 Mbps	10 Mbps	10 Mbps
Longitud Máxima del segmento	500 m	185 m	500 m	100 m	1800 m
Longitud Total de la red	2500 m	925 m	2500 m	500 m	3600 m

Tabla 2.5.5.3 Especificaciones del nivel físico IEEE 802.3

Resumen estándar IEEE802.3

El estándar IEEE 802.3 define el protocolo de acceso al medio CSMA/CD para la topología en bus. Ethernet e IEEE802.3 a pesar de su diferencia en la estructura de tramas son compatibles en el mismo medio físico. La norma comprende el nivel MAC y el nivel físico.

- **Estándar IEEE 802.3u. Fast Ethernet (100Mbps)**

Las redes LAN con tecnología Ethernet cumplieron durante mucho tiempo con las exigencias de ancho de banda en la mayoría de los casos, pero con el desarrollo de la informática, de los sistemas operativos basados en interfaces graficas que exigen mas recursos de hardware, asimismo las aplicaciones cada vez más complejas y capaces de manejar archivos de gran tamaño hacen que las redes Ethernet de 10 Mbps se conviertan en un cuello de botella para las cantidades enormes de trafico circulando por la red. Debido a esto surgió la nueva especificación de Ethernet que permite un ancho de banda de 100Mbps. Para aumentar la velocidad de la red de 10 Mbps a 100 Mbps se han definido nuevos especificaciones de Ethernet denominadas en conjunto FastEthernet (IEEE802.3u). La nueva especificación para ethernet de alta velocidad o Fast Ethernet fue desarrollada por el grupo de trabajo 802.3u.

Fast Ethernet se creo tratando de satisfacer los requerimientos de los nuevos modelos y para dar respuesta a la demanda de mayores anchos de banda, permitiendo así las conexiones de nuevas aplicaciones como bases de datos, o aplicaciones cliente servidor, además de la gran ventaja que representa el pequeño gasto de actualización a Fast Ethernet comparada con FDDI o ATM, aunado a lo anterior mantiene una total compatibilidad e interoperabilidad con Ethernet. Todas estas ventajas y compatibilidades se dieron debido a que el objetivo del grupo de trabajo 802.3u era obtener alta velocidad en redes de área local adaptando el

estándar IEEE 802.3 para CSMA/CD a la velocidad de 100 Mbps. Se conservo el método de acceso MAC con el objeto de mantener la máxima compatibilidad con la extensa base instalada de redes Ethernet e IEEE 802.3.

Así el estándar IEEE 802.3u se refiere a cualquiera de las varias especificaciones de ethernet de 100 Mbps (100BaseTX, 100BaseFX, 100BaseT4). Fast Ethernet ofrece un aumento de velocidad diez veces mayor que el de la especificación de ethernet 10BaseT, presenta características tales como formato de trama, mecanismos MAC y MTU similares. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes de Fast Ethenet. En suma esta especificación esta basada en una extensión de la especificación IEEE802.3

La primera cuestión que se replanteo para incrementar la velocidad era la relación entre el tiempo de spot y la máxima distancia de operación de las redes CSMA/CD, la distancia máxima puede ser determinada por la atenuación del cable o por el tiempo de spot. Para una longitud máxima de 2.5 Km se tiene aproximadamente un retardo de la señal de 25 microsegundos. Se fijo un retardo máximo de 50 microsegundos para poder detectar las colisiones antes de la transmisión de toda la trama. En este tiempo se pueden transmitir 500 bits a 10 Mbps, por lo que la trama de Ethernet mínima se fijo en 512 bits o sea 64 bytes u octetos.

En Ethernet a 100 Mbps con operación en semiduplex la distancia entre estaciones se fija en 200 m, siendo de 100 m la distancia entre estación y hub.

Fast ethernet se dio gracias a sus dos grandes características: Transmisión full duplex y autonegociación:

Inicialmente en el Ethernet de medio compartido por cable coaxial se realizaba una comunicación half-duplex, así una estación transmitía mientras las demás escuchaban por lo cual se tenia que usar el protocolo de acceso al medio CSMA/CD, para que una estación pudiera transmitir solo cuando el canal estaba desocupado.

La aparición del cableado 10BaseT permitió la capacidad de separar las trayectorias de transmisión y recepción de datos. De esta forma el cable UTP nos ofrece 8 cables de los cuales un par se utiliza para la transmisión y el otro para la recepción. Debido a lo anterior ya no se requiere la función de escucha de portadora puesto que el cable se utiliza para transmitir y recibir solo con un nodo. Aunado a esto la aparición del ethernet switcheado trajo como consecuencia que el canal de transmisión ya no se compartiera con varios usuarios lo que permite la conexión entre switches o entre switch y host en una conexión punto a punto, como las colisiones solo ocurren en un medio compartido ya no se requieren las funciones de detección de colisiones y los algoritmos de espera.

La especificación 100BaseT describe un proceso de autonegociación que permite a los dispositivos a cada extremo intercambiar información y configurarse automáticamente para trabajar a la máxima velocidad, es decir negocian si se conectan a 10 o 100 Mbps. La autonegociación se realiza por medio de un Pulso de Enlace Rápido (FLP) con el cual se identifica la tecnología de capa física. Esta función de autonegociación también permite descubrir si la transmisión será 10BaseT half o full duplex, 100BaseT half o full duplex y 100BaseT4. Se puede hacer el reconocimiento aun cuando un extremo no tenga la capacidad de autonegociación.

100BaseT es el nombre genérico empleado para la utilización de cable de pares para transmitir en banda base manteniendo las características de 10BaseT. La conexión entre hub y estación es punto a punto y la distancia máxima es de 100 metros. La tabla 2.5.5.4 muestra las diferentes modalidades de 100BaseT.

Tecnología	Operación	Cable	Distancia
100BaseTX	Full/Semiduplex	UTP CAT-5, 2 pares	100 m
100BaseT4	Semiduplex	UTP CAT-3, 4 pares	100 m
100BaseT2	Full/Semiduplex	UTP CAT-3, 2 pares	100 m
100BaseFX	Full/Semiduplex	MMF 62.5/125	130m, 160m 400 m, 2 Km

Tabla 2.5.5.4 Diferentes modalidades de la tecnología 100BaseT

En la tabla se incluye el medio físico de fibra óptica, en el cual la distancia entre conmutadores en operación semiduplex alcanza los 400 m, mientras que en operación duplex llega a 2 Km

En paralelo al desarrollo de Fast Ethernet se desarrollo la conmutación de capa 2, la cual desarrolla las funciones de un puente por hardware lo que posibilita que un gran numero de puertos estén activos simultáneamente y proporcionen auto negociación 10/100 Mbps individualmente por puerto. También suelen incorporar otras características por hardware como es la clasificación de tráfico, marcado de VLAN y gestión de red.

Las ventajas del estándar Fast Ethernet son entre otras que la migración de Ethernet a Fast Ethernet es transparente ya que Fast Ethernet usa los mismos protocolos, aplicaciones, drivers etc., si el cableado esta estandarizado (UTP categoría 5) no se requiere actualización de este, continua usando 2 pares de hilos UTP categoría 5 como lo hace Ethernet, a diferencia de 100VG-AnyLan que necesita 4 pares, además que su esquema de cableado de tipo estrella, lo que facilita la detección de problemas. Uno de los problemas que puede tenerse para implementar Fast Ethernet es que el cableado no se encuentre dentro de los estándares y que sea de una categoría por debajo de la 5.

Las topologías posibles con Fast Ethernet quedan reducidas a la topología en estrella.

- **Estándar IEEE 802.3z Gigabit Ethernet**

El estándar IEEE 802.3z define las especificaciones del Gigabit ethernet. Gigabit Ethernet es resultado de la evolución de la tecnología Ethernet a 100 Mbps. Aunque ATM puede cumplir con los requerimientos de mayor ancho de banda de las aplicaciones modernas presenta cambios de arquitectura y de trama, mientras que Gigabit Ethernet proporciona una migración sin discontinuidades.

Junto al desarrollo de Gigabit ethernet se comenzó a desarrollar el concepto de conmutación de capa 3, la cual es una evolución de los encaminadores para que puedan ser acelerados mediante hardware. Normalmente solo se optimizan las funciones relacionadas con el protocolo IP.

Para que Ethernet pueda operar a 1 Gigabit se tiene que resolver el problema de la relación entre la duración del spot y la distancia máxima, manteniendo la longitud mínima de trama de 64 bytes para tener la compatibilidad con las redes de velocidad inferior de 10 y 100 Mbps. Para esto se introdujo el concepto de carrier extensión o extensión de la portadora, con lo cual se mantiene la longitud de la trama mínima de 512 bits, pero si cuando una estación realiza una transmisión la trama es menor que el tiempo del spot se mantiene el estado de transmisión y la capa física mantiene una secuencia de símbolos especiales después de los 4 bytes del campo FCS hasta alcanzar el fin del tiempo del spot. Si se detecta una colisión ya sea en la transmisión de la trama o en la transmisión de los símbolos

de portadora extendida, el transmisor interrumpe la transmisión y manda los 32 bits de señal de congestión o jam.
Este procedimiento es poco eficiente para tramas cortas por lo que para este tipo de tramas se usan las ráfagas de tramas. Con las ráfagas de tramas el transmisor, al terminar de enviar la primer trama con éxito incluida la extensión de portadora y si no se producen colisiones, continua transmitiendo tramas adicionales si es que hay mas hasta que expira un contador llamado contador de ráfagas.
Para la capa física el estándar IEEE 802.3z define el uso de fibra y par de cobre. Las opciones de cableado son:

- Fibra óptica multimodo (1000BaseSx y 1000Base LX) Sx utiliza una frecuencia de 850 nm y LX usa 1330nm. Un cable de 62.5 micras cubre un máximo de 300 metros (en la especificación Sx) o 500 metros (en la especificación Lx). Un cable de 50 micras cubre una distancia de 550 metros (para las dos especificaciones Sx y Lx)
- Fibra óptica monomodo (1000BaseLx). La máxima distancia que soporta Gigabit ethernet es de 3000 metros haciendo uso de este cable. El incremento de la distancia sobre el soporte de la FO multimodo es la baja dispersión.
- Cable de cobre (UTP/1000BaseT) Este tipo de cable esta definido por la especificación 802.3ab, considerando un cable de categoría 5, la máxima distancia para Gigabit ethernet será de 100 metros. Esta se basa en un cable de 4 pares.

La tabla 2.5.5.5 muestra los medios físicos y distancias para IEEE 802.3z

Tecnología	Cable	Distancia
1000BaseT	UTP-5 mejorado (UTP-6)	100 m
1000BaseX	Fibra óptica 850 nm y 50/62.5	220m a 550m
1000BaseCX	Twinax	25 m
1000BaseLX	Fibra óptica SMF de 1300 nm	5 km

Tabla 2.5.5.5 Medios físico y distancias para IEEE 802.3z

La capa MAC. Estándar IEEE802.3z.
La capa MAC para Gigabit ethernet es idéntica a la de ethernet y Fast ethernet, con la excepción que usa una forma simple de control de flujo especificado en el estándar 802.3x. Un dispositivo puede enviar un comando que diga al dispositivo final que termine la transmisión y más tarde enviara un comando que indique si otro dispositivo puede iniciar el envío nuevamente.

- **Estándar IEEE 802.4. Control de acceso al medio MAC con paso de testigo en bus. Token bus**

La norma IEEE 802.4 define el protocolo de control de acceso al medio MAC para paso de testigo en bus (Token Bus) así como opciones sobre medios de transmisión y velocidades de red. El objetivo de este estándar además de simplificar las redes en bus es garantizar un tiempo máximo de retardo.
La forma de operación es la siguiente: Las estaciones están conectadas físicamente un bus (cable lineal formado con cable coaxial de 75 ohm) pero en su operación forman un anillo

lógico, por lo que cada estación tiene asignada una posición lógica independiente de la física, dentro de una secuencia ordenada y circular, Fig. 2.5.5.13.

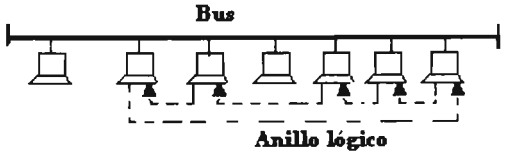


Fig. 2.5.5.13 Red paso de testigo en bus

Cada estación conoce la dirección de las estaciones a su izquierda y derecha, es decir, conoce la dirección de su antecesora (EA) y la que le sigue (ES). El derecho de acceso al medio se regula con una trama de control llamada testigo o token. Cuando el anillo lógico se inicia, el dispositivo que tiene la prioridad mayor es el que puede enviar la primer trama.
La estación que posee el token obtiene el control del medio durante un periodo de tiempo determinado. Durante ese tiempo puede transmitir todas sus tramas, consultar estaciones y recibir respuestas. Finalizada la transmisión o el tiempo asignado cede el testigo a la siguiente estación en el orden lógico, la cual ahora tiene permiso para transmitir. La operación de este método consiste en alternancias de transmisión y transferencias de testigo.
El token se propaga alrededor del anillo lógico, de forma que solo su poseedor esta autorizado a transmitir tramas. Como solamente un dispositivo puede tener el token a la vez, no hay posibilidad de colisiones. Este método de acceso al medio se conoce con el nombre de Token-Passing (paso de testigo).
Cuando los dispositivos se activan por primera vez no están dentro del anillo, de tal forma que el protocolo MAC tiene la capacidad para agregar y retirar dispositivos del anillo.
Las estaciones que no tienen el token están conectadas para responder a consultas o peticiones de confirmación.
Se pueden manejar velocidades de 1, 5 y 10 Mbps. La capa física en su totalidad es completamente incompatible con la norma 802.3.
Las direcciones de las estaciones EA y ES se determinan dinámicamente para determinar un único anillo lógico. Este anillo se crea y mantiene de manera que las estaciones se ordenen lógicamente por orden descendente de sus direcciones MAC. Las funciones generales del subnivel MAC son las siguientes:

- Temporización para detectar la perdida del testigo.
- Inicio de la transmisión.
- Tiempo de posesión del testigo.
- Limitación de datos en el bus.
- Reconocimiento de dirección de nodos.
- Encapsulado de tramas (incluyendo preparación de testigo).
- Generación de FCS y verificación.
- Reconocimiento de testigo valido.
- Adición de nuevos miembros al anillo.
- Recuperación de errores en un nodo.

El estándar IEEE 802.4 incluye los siguientes elementos del nivel MAC y del nivel físico:

- Subnivel MAC
- Especificaciones de servicio MAC

Definen el servicio proporcionado por el IEEE802.4 al LLC o a cualquier otro usuario de nivel superior, incluyendo facilidades para la transmisión y recepción de PDU y suministran información del estado de las operaciones. También describen la estructura de trama y las interacciones que tienen lugar entre las entidades MAC.

- Protocolo y unidades de datos MAC

• Nivel físico

- Especificaciones de servicio

Definen el conjunto de servicios proporcionados por el nivel físico al nivel MAC. Cada especificación de la entidad de nivel físico incluye las características funcionales, eléctricas y mecánicas necesarias para la transmisión y recepción de señales sobre un determinado medio.

- Especificaciones del medio físico

Define las características del medio físico, sus componentes y el cable utilizados para la conexión de la estación al medio.

Estructura de la trama MAC. Estándar IEEE802.4.

La especificación describe la estructura de la trama y las interacciones que tiene lugar entre las entidades MAC, la Fig. 2.5.5.14 muestra el formato de la trama del protocolo IEEE 802.4.

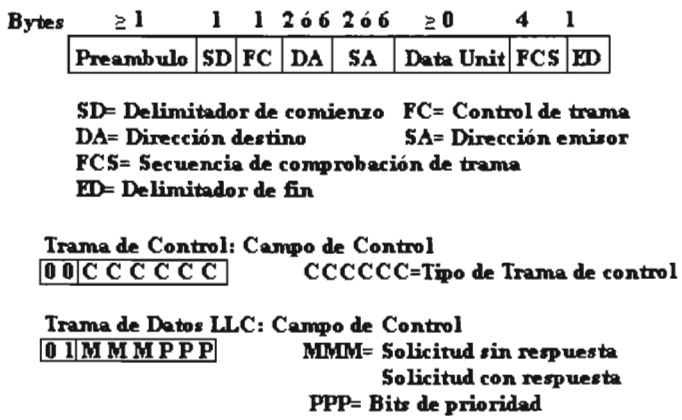


Fig. 2.5.5.14 Formato de la trama MAC IEEE 802.4

Los campos de la trama son:

- Preámbulo. El preámbulo es un patrón de 1 o más octetos utilizado por el receptor para establecer la sincronización de bit
- Delimitador de trama. Indica el comienzo de la trama. Contiene patrones de señalización distintos a los datos. Su codificación es XX0XX000, X es un símbolo carente de información, la forma de este símbolo depende de la codificación de señal utilizada en el medio.
- Trama de control. Los dos primeros bits del control de trama indican si se trata de una trama de control o de una trama de datos LLC. Las tramas de control se emplean para gestionar el protocolo de testigo en bus. Los 6 bits restantes identifican su identidad. En una trama de datos LLC tres bits indican el tipo de trama: solicitud sin confirmación, solicitud con confirmación.
- Dirección destino: Dirección hacia la cual va dirigido el paquete. Puede ser de 2 o 6 bytes.

- Dirección origen: Dirección de la estación desde la que se envía el paquete.
- Datos: Contiene la unidad de datos LLC o información para control del modo de operación.
- Secuencia de verificación de trama: Es el código de dispersión de 32 bits de los datos, el cual usa un algoritmo de verificación de redundancia cíclica (CRC) para generar este campo de 4 octetos sobre la base del polinomio generador.

Las funciones básicas de gestión y mantenimiento del acceso al medio que se realiza por al menos una estación son las siguientes:

- Adición al anillo para que las estaciones no participantes en el anillo deban tener periódicamente la oportunidad de incorporarse al mismo.
- Eliminación del anillo, para que una estación sea capaz de retirarse del anillo por sí misma.
- Iniciación del anillo. Cuando se arranca la red o se recupera de una falla debe haber un mecanismo descentralizado que decida el orden de iniciación del anillo.
- Recuperación del token cuando haya pérdida del mismo.

El esquema de prioridades en el estándar token bus se aplica sobre los datos que se transmiten, para ello se tienen cuatro niveles de prioridad que en orden descendente son: 6, 4, 2, 0. El objetivo es gestionar la totalidad del ancho de banda de la red en función de las tramas más prioritarias y transmitiendo las tramas menos prioritarias siempre que exista ancho de banda suficiente. Un temporizador limita el tiempo máximo durante el cual una estación puede poseer el testigo. Así cuando una estación recibe el token empezara a transmitir sus tramas de mayor prioridad sin exceder el temporizador, si termina de transmitir la trama de mayor prioridad y le queda tiempo puede empezar a transmitir las de menor prioridad.

Especificaciones del nivel físico. Estándar IEEE802.4.

El estándar IEEE802.4 defina cuatro posibles alternativas de medio físico las cuales se observan en la Fig. 2.5.5.15

Parametro	Carrierband fase continua	Carrierband fase coherente	Banda ancha	Fibra optica
Velocidad	1 Mbps	5 y 10 Mbps	1, 5 y 10 Mbps	5,10 y 20 Mbps
Ancho de banda	NA	NA	1.5, 6 y 12 Mhz	270 nm
Modulación de frecuencia	Manchester FSK continuo	FSK fase coherente	Multinivel AM/FSK	On-off
Topología	Bus omni-direccional	Bus omni-direccional	Bus direccion-al (árbol)	Estrella pasi-va o activa
Medio	Cable coaxial 75 ohm	Cable coaxial 75 ohm	Cable coaxial 75 ohm	Fibra optica

Fig. 2.5.5.15 Medios alternativos del nivel físico IEEE 802.4

- La alternativa Carrierband de fase continua como todas las redes carrier band dedican la totalidad de la capacidad del medio a una única transmisión de señales analógicas, realizan una transmisión bidireccional y emplean la modulación FSK que a bajas frecuencias tiene una menor atenuación, previamente codificada la información digital a transmitir mediante el código Manchester.
- Carrierband de fase coherente se denomina así por que los puntos que cruzan el cero están en fase tanto al comienzo como al final de cada uno de los tiempos de un bit. En la codificación empleada el 1 binario se representa por una frecuencia igual a la

velocidad de transmisión mientras que el 0 se representa por una frecuencia igual al doble de la velocidad de transmisión. Así si la velocidad de transmisión es de 5 Mbps, las frecuencias correspondientes al 1 y 0 respectivamente son 5 y 10 Mhz.

- En la alternativa de fibra óptica la especificación del ancho de banda y la portadora se realiza en términos de longitud de onda en lugar de frecuencias. La técnica de modulación es un tipo de desplazamiento de amplitud ASK conocido como modulación por intensidad. Para evitar problemas de sincronización con largas series de 1's y 0's se realiza una codificación Manchester con lo que el 0 se transmite como un pulso de luz seguido de la ausencia de pulso y el 1 como la ausencia de un pulso seguido de un pulso de luz, así la velocidad efectiva de señalización se duplica por lo que las velocidades de transmisión de 5, 10 y 20 Mbps requieren velocidades de señalización óptica de 10, 20 y 40 Mbaudios.

Principales características del estándar IEEE 802.4:

- Se constituye con un bus de banda ancha.
- Cable coaxial de 75 ohms.
- Velocidad de transmisión de 1.5 o 10 Mbps.
- La configuración física de la red es del tipo bus, pero funciona como un anillo lógico.
- Cada estación conoce la identidad de las estaciones anterior y posterior.

- **Estándar IEEE 802.5 Control de acceso al medio MAC con paso de testigo en anillo. Token Ring.**

La norma de anillo IEEE 802.5 o estándar Token Ring tiene una topología física en anillo y su método de acceso al medio se basa en el Token Passing o paso de testigo.
La red de paso de testigo en anillo consiste en un conjunto de estaciones conectadas por un medio de transmisión, Fig. 2.5.5.16

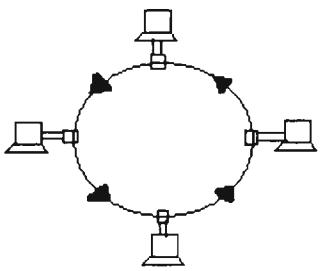


Fig. 2.5.5.16 Red paso de testigo en anillo.

En la operación de la red de paso de testigo en anillo, la información se transmite secuencialmente bit a bit desde una estación activa a la siguiente. Cada estación activa regenera y repite cada bit. La estación que tiene el derecho de acceso al medio introduce la información en el medio donde la información circula pasando por las estaciones. La estación destino de la información copia los datos al mismo tiempo que los pasa a la red. Finalmente la estación emisora retira la información del anillo. Las estaciones obtienen el derecho a transmitir su información cuando detectan un testigo o token en el medio. El testigo es una señal de control compuesta por una secuencia especial de bits que circula por el anillo cuando todas las estaciones están inactivas. De esta forma cualquier estación tras detectar el testigo lo captura modificándolo y convirtiéndolo en el comienzo de una trama al cual le añade los campos de control y estado, de direccionamiento, información, secuencia de comprobación de trama y secuencia de finalización de trama.

En las interfaces de anillo hay dos modos de operación, uno para escuchar y otro para transmitir.
En el modo de escucha cada uno de los bits que llegan a una interfaz se copia en una memoria temporal para después copiarse de nuevo sobre el anillo. Mientras el paquete se encuentre en la memoria temporal puede inspeccionarse y modificarse antes de ser escrito nuevamente sobre el anillo. Durante la inspección el dispositivo verifica la dirección que tiene el paquete de datos y en caso de que sea su dirección lo procesa.
En el modo de transmisión que solo ocurre después de que el token ha sido capturado, la interfaz rompe la conexión existente entre su entrada y su salida para introducir sus propios datos al interior del anillo.
Al terminar su transmisión de información y después de las operaciones de comprobación de errores la estación emisora inicia un nuevo testigo, para proporcionar la oportunidad de obtener el acceso a la red a las demás estaciones del anillo. Cuando él ultimo bit del marco haya recorrido la trayectoria y haya regresado, se deberá retirar y la interfaz deberá conmutarse inmediatamente al modo de escucha para evitar perder el token y tener la posibilidad de volver a transmitir en caso de que ningún otro dispositivo lo haya escogido.
Un temporizador de posesión de testigo controla el periodo máximo que una estación ocupa el medio antes de pasar el testigo.
Se pueden definir niveles de prioridad mediante un acuerdo entre los usuarios de la red.
La red proporciona mecanismos de recuperación y detección de errores con la finalidad de asegurar el estado normal de funcionamiento en caso de que los errores de transmisión o perturbaciones en el medio provoquen el incorrecto funcionamiento del método de acceso.
La detección y recuperación de errores la realiza una estación a través de una función de monitorización de la red.
Las redes en anillo basan su buen funcionamiento en tres funciones básicas: inserción de datos, recepción de datos y retirada de datos. Estas funciones son realizadas por los repetidores que sirven como punto de conexión de las estaciones a la red. El repetidor recoge de la red las tramas que representan a los datos y verifican la dirección de destino, si la estación conectada a ese repetidor reconoce la dirección como suya se copia el resto de la trama. La retirada de las tramas en un anillo es más difícil que en el bus o árbol ya que en estos últimos al propagarse la señal cuando llega a los terminadores es absorbida y eliminada con lo que al poco tiempo de realizada la transmisión el medio queda limpio de datos. En el anillo debido a que es un bucle cerrado las tramas circularan indefinidamente hasta que sean retiradas, lo cual puede realizarse por el repetidor destino o por el emisor una vez que hayan completado una vuelta al anillo. El último caso es más aconsejable por que además de que hace un reconocimiento automático permite la transmisión de multicasting para que un paquete sea enviado a varias estaciones.
El repetidor puede encontrarse en dos estados de funcionamiento: escucha y transmisión. En el estado de escucha cada uno de los bits es retransmitido tras un pequeño retraso necesario para que el repetidor realice sus funciones de análisis de los bits para reconocer los patrones de la dirección y de control de testigo que otorga el permiso para transmitir, también debe copiar cada bit de la trama dirigida a su estación y al mismo tiempo enviarlo a la red. El repetidor pasa al estado de transmisión cuando la estación conectada tiene datos para transmitir y se tiene permiso para transmitir.
La señal que circula por un medio de transmisión en anillo incluye algún tipo de sincronización como el que se obtiene usando por el ejemplo la codificación Manchester

Diferencial. Cuando los datos que circulan por el anillo llegan al repetidor este recupera la información de sincronización con dos propósitos:
1) Para conocer cuando tomar las muestras de la señal que llega para recuperar los bits de datos.
2) Utilizar esta información para transmitir la señal al siguiente repetidor.
Cuando el repetidor emite los datos, lo hace mediante una señal limpia sin distorsión. Debido al efecto del jitter (desviación en el tiempo de recuperación del sincronismo) el ancho del pulso digital se expandirá y contraerá aleatoriamente a medida que la señal viaje por el anillo y se producirá una acumulación de la desviación en el tiempo de recuperación del sincronismo, esto causa que la latencia o longitud en bits del anillo varié provocando que se pierdan o retransmitan bits si la latencia disminuye o que se retransmitan mas si la latencia aumenta.
El estándar IEEE 802.5 define los servicios y protocolos de control de acceso al medio para redes que operan con paso de testigo en anillo. Define también los servicios y la especificación del nivel físico. Los componentes del estándar son:

- Subnivel MAC
- Especificaciones de servicio MAC
- Protocolos y unidades de datos MAC
- Nivel físico
- Especificaciones de servicio
- Especificaciones independientes del medio
- Especificaciones del medio físico.

En la Fig. 2.5.5.17 tenemos los formatos de testigo y de la trama definidos por el protocolo IEEE802.5

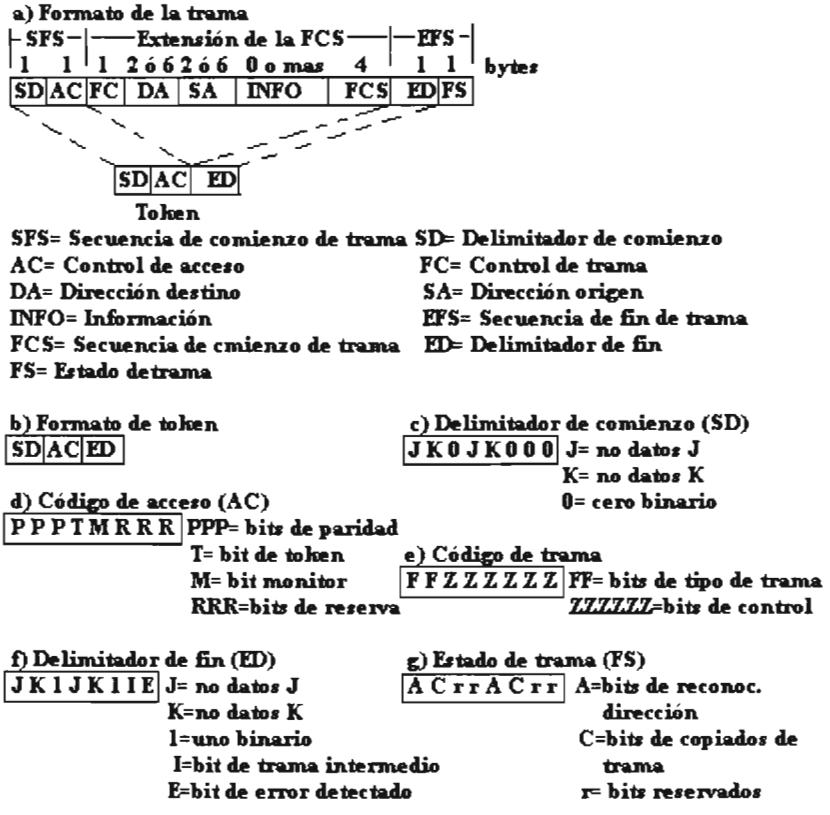


Fig. 2.5.5.17 Formato de la trama IEEE 802.5-Token Ring

De la Fig. 2.5.5.17 podemos observar que la trama Token Ring es parecida a la de Ethernet con la diferencia que a los datos se les agrega un token que es el que marca la prioridad de transmisión.

Los campos que contiene la trama son los siguientes:

- Delimitador de comienzo SD (Starting Delimiter): Indica el comienzo del testigo o de la trama, es un patrón distinguible de los datos, en el formato JK0JK000, J y K son símbolos que representan la ausencia de datos.
- Control de acceso AC (Access Control): Contiene los bits de prioridad y reserva utilizados en el mecanismo de prioridad y el bit de monitorización empleado en el mecanismo de mantenimiento. Contienen también el bit de testigo que indica si se trata de un testigo o de una trama. En el caso de ser un token o testigo solo se acompaña de un campo más el delimitador de trama.
- Control de trama FC (Frame Control): indica si la trama contiene datos LLC o es una trama de control MAC. En este último caso los bits de control indican el tipo de trama MAC.
- Dirección de Destino DA: Especifica la(s) estación(es) a la(s) que va dirigida la trama. Puede ser una dirección MAC (una estación), dirección de grupo (varias estaciones) o una dirección global (todas las estaciones del anillo).
- Dirección origen SA: Especifica la dirección de la estación que envío la trama.

- Información I: Contiene los datos en el caso de una trama de datos o un vector MAC si es una trama MAC.
- Secuencia de comprobación de trama FCS: comprobación de redundancia cíclica de 32 bits basada en los campos FC, DA, SA e I.
- Delimitador de final ED. Contiene los símbolos J y K para indicar el final de trama, incluye los bits E e I con el significado mostrado en la tabla 2.5.5.6.

BIT	Descripción Control de Acceso
Prioridad (PPP)	Prioridad del Token
Token (T)	0 en un token, 1 en una trama
Monitor (M)	Prevención de tramas o token persistentes
Reserva (RRR)	Usado para pedir que el siguiente token se emita Con la prioridad requerida
	Control de Trama
Tipo de trama (FF)	Trama MAC o LLC
	Delimitador final
Trama intermedia I	0 indica última trama o solo trama de transmisión
	1 indica que siguen mas tramas
Error detectado (E)	Fijado por cualquier estación que detecta un error
	Estado de trama
Recon. dirección A	La estación ha reconocido su dirección
Copiado de trama C	La estación ha copiado la trama

Tabla 2.5.5.6 Bits de control de la trama MAC IEEE 802.5

- Estado de trama FS (Frame Status): contiene los bits A y C con su significado mostrado en la tabla 2.5.5.6. Estos bits están fuera del ámbito del FCS por lo que se duplican para proporcionar una comprobación de error.

Token ring tiene definidas dos velocidades:

- La velocidad es de 4 Mbps cuando se usa el método de liberación normal del token. En este método cuando la trama de datos ha pasado por cada estación del anillo, regresa a la estación origen y el token es liberado.
- La velocidad es de 16 Mbps cuando se usa una liberación temprana del token. En este método cuando los datos son enviados sobre el anillo el token es inmediatamente liberado y pasa a la siguiente estación.

En esta tecnología se usan dos medios de transmisión el STP de dos pares que no es estándar y el UTP, STP o FTP de 4 pares estandarizado con RJ45.

La topología de Token Ring es una configuración lógica, pues físicamente una topología en anillo cerrado no existe, es en realidad una topología en estrella gracias al dispositivo MAU (Multistation Access Unit- Unidad de Acceso de Multiples Estaciones) localizado en el centro de la estrella al que se conectan ya sea por par trenzado o por fibra óptica todas las estaciones y en cuyo interior es donde realmente se estructura de manera lógica el anillo.

Las principales características del nivel físico del estándar IEEE802.5 son:

- Transmisión en banda base.
- Velocidad de transmisión de 1.4 o 16 Mbps.
- Utiliza cable de par trenzado blindado de 150 ohms.

- Topología en anillo con cableado en estrella.
- Numero máximo de estaciones: 260 con un puente se pueden agregar otras 260.
- La distancia máxima desde una estación hasta la MAU puede estar alrededor de los 100 metros.

- **Estándar FDDI**

La Interfaz de datos distribuidos por fibra FDDI es un estándar para redes de alta velocidad. Sus principales características son:

- Red basada en fibra óptica.
- La velocidad de transmisión es de 100 Mbps.
- Utiliza una configuración en anillo.
- Soporta distancias de hasta 2 Km entre estaciones y una circunferencia total de fibra de 200 Km
- El numero máximo de estaciones conectadas es de 500.
- Normalmente se usa para unir el concentrador que conecta varias estaciones a un servidor muy potente.
- Su método de acceso al medio es el paso de testigo.

- **Estándar IEEE 802.11**

El fundamento de muchas de las redes inalámbricas se encuentra basado en el estándar IEEE 802.11 y más concretamente en la especificación IEEE 802.11b, con este estándar se garantiza la interoperatividad entre fabricantes consiguiendo al mismo tiempo una significativa reducción de costos y abaratamiento de dispositivos para el usuario final.
Inicialmente en el IEEE 802 se formo el grupo de trabajo IEEE 802.11 que tenia como objetivo generar una norma para las redes inalámbricas WLAN.
El instituto de normalización Europeo ETSI creo una norma llamada HiperLAN (High Performance LAN) para asignar las bandas de 5.2 y 17.1 GHz.
La asociación IRDA (Infrared Data Association) promovió el desarrollo de las WLAN basadas en enlaces infrarrojos.
El forum de redes inalámbricas WLI Forum (Wireless LAN Interoperability Forum) se creo para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos.
El consorcio WECA (Wireless Ethernet Compatibility Alliance) estableció un estándar llamado Wi-Fi que permite la certificación de los productos apegados a esta norma para que exista compatibilidad, así como aspectos de facilidad de configuración, unanimidad de protocolos, modos de funcionamiento y otros.
Como la intención del IEEE 802.11 era permitir la conexión de dos sistemas diferentes y de marcas diferentes de manera que pudieran intercambiar datos sin preocuparse por definir otros elementos como los protocolos de transmisión o de red, se trabajo tan solo en la capa física y en la capa de enlace de datos, de la capa de enlace de datos solo se trabajo sobre la subcapa MAC.

El IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa (DSSS) en la banda de frecuencia 2.4 GHz ICM.

- Espectro expandido por salto de frecuencias (FHSS) en la banda de frecuencia 2.4 GHz ICM.
- Luz Infrarroja en banda base.

La capa MAC soporta tres topologías básicas:

- Servicio básico independiente IBSS (Independent Basic Service Set). Esta configuración es semejante a una red punto a punto en la que no se requiere que ningún nodo específico funcione como servidor. Las implementaciones con esta topología cubren un área limitada y no están conectadas a ninguna otra red más grande, también se le llama red ad hoc.
- Servicio basico BSS (Basic Service Set). Esta configuración consta de un nodo central o punto de acceso (AP) que actúa como centro de transmisión para una única celda inalámbrica por la que ha de pasar necesariamente cuando se establece comunicación entre dos estaciones. Este punto de acceso se necesita para disponer de las facilidades especificadas por el estándar (por ejemplo conectar el segmento inalámbrico a la red cableada). Es conocida también como red basada en infraestructura.
- Servicio básico extendido ESS (Extended Service Set). Esta configuración consiste de múltiples celdas BSS que pueden unirse a través de cables o de forma inalámbrica, también se le llama sistema de distribución.

Como método de acceso al medio se tiene el CSMA/CA (Acceso múltiple por detección de portadora evitando colisiones) el cual se diferencia del utilizado por Ethernet ya que realiza un uso más eficiente del ancho de banda. Este protocolo tiene el problema de que alguna estación en un momento dado no sea escuchada por alguna estación y las demás si, por lo que la estación que no escucha la transmisión puede intentar transmitir. Para evitar este problema se agrego al protocolo CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento de mensajes positivo llamado Reservation-Based Protocol. Su funcionamiento es como se describe a continuación:

Cuando una estación esta lista para transmitir primero envía una solicitud al punto de acceso RTS (Request to Send), quien difunde el NAV (Network Allocation Vector=tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS) a todos los demás nodos para informarles que se va a empezar a transmitir y por lo tanto ellos no lo hagan, también se le indica cual va a ser la duración de la transmisión. Los nodos dejaran de transmitir durante el tiempo indicado por el NAV mas un intervalo extra de tiempo de retroceso (backoff) aleatorio. Si no encuentra problemas el punto de acceso responde con una autorización (CTS-Clear to Send) que permite al solicitante enviar su trama con los datos. Cuando el punto de acceso ha recibido correctamente la información envía una trama de reconocimiento (ACK-Acknowledgement) notificándoselo al transmisor.

Con respecto a la seguridad el estándar cubre dos aspectos que son la autentificación y la privacidad.

- Autentificación. La autentificación consisten en proporcionar y verificar la identidad de una estación o cliente. Debido a que los dispositivos que funcionan con el estándar IEEE 802.11 operan en un sistema abierto, donde cualquier cliente inalámbrico puede asociarse a un access point sin ninguna comprobación por parte de este se requiere aplicar algún sistema de autentificación. Para la autentificación se utiliza WEP (Wired Equivalent Privacy), WEP configura una clave en el punto de acceso y sus estaciones. Puede usarse WEP-40 o WEP-128 dependiendo del

número de bits que se quiera usar en la clave. Solo los dispositivos con una clave valida pueden estar asociados a un determinado access-point.

- Privacidad. Normalmente en la comunicación inalámbrica los datos son enviados por default sin ninguna encriptación, con WEP los datos pueden ser encriptados antes de ser enviados inalambricamente, para realizar esto se usa el algoritmo de encriptación RC4 (RC4 es un algoritmo de encriptación de 40 o 128 bits desarrollado por RSA Data Security). La misma clave usada para la autentificación es usada para encriptar y desencriptar los datos.

El estándar define dos modos de administración de potencia:

- Activo. En el modo activo el cliente transmite y recibe normalmente.
- Espera. Cuando no hay actividad el cliente entra en modo descanso y por lo tanto no puede transmitir ni recibir. Para evitar problemas de red se tiene una memoria intermedia en la que se almacenan los datos para que el cliente los pueda recoger periódicamente.

También el estándar permite la movilidad (roaming) para que las estaciones puedan moverse mas allá del área cubierta por su Access-Point pudiéndose reasociar con un nuevo Access-Point al que previamente envía una solicitud (Reassociation Request).

El estándar trata básicamente dos tecnologías de transmisión:

- La tecnología de infrarrojos.
- La tecnología de radiofrecuencia.

- **Tecnología de infrarrojos.**

Las características que menciona el IEEE 802.11 son:

- Transmisión infrarroja difusa.
- El receptor y transmisor no tienen que ser dirigidos uno contra el otro y no necesitan una línea de vista limpia.
- La distancia máxima entre equipos es de 10 metros.
- Utilización únicamente en edificios.
- El acceso básico se corresponde con 1 Megabaudios de velocidad de transmisión y modulación de 16 posiciones PPM (Pulse Position Modulation) pudiendo conseguir una tasa de datos de 5 Mbps.
- El acceso avanzado se corresponde con 2 Megabaudios de velocidad de transmisión y modulación en 4 posiciones PPM pudiendo conseguir una tasa de datos de 10 Mbps.
- El rango de longitudes de onda permitido es de 850 a 950 nm.

Los sistemas de transmisión infrarroja difusa permiten que el transmisor no tenga que estar alineado con el receptor. Así una topología muy común para redes inalámbricas con tecnología infrarroja consiste en colocar en el techo un access point hacia el cual se dirigen los dispositivos inalámbricos y desde el cual es difundida la señal hacia esos mismos dispositivos.

El funcionamiento de la capa física se basa en un dispositivo emisor LED el cual emite la luz que se propaga en el espacio libre. El receptor es un fotodiodo PIN que recibe los pulsos de luz y los convierte en señales eléctricas que tras su manipulación (amplificación, conversión a formato bit y retemporización) pasan a la UART del computador. En el proceso de transmisión los bits viajan mediante haces de pulsos, donde el cero lógico se representa con la existencia de luz y el 1 con la ausencia de luz. El enlace entre los

extremos es punto a punto con un cono de apertura de 30°, siendo la transmisión del tipo semiduplex.
En la capa de enlace se utiliza el protocolo IrLAP (Infrared Link Access Protocol). Este protocolo se encarga de gestionar las tareas relacionadas con el establecimiento, mantenimiento y finalización del enlace entre los dos dispositivos que se comunican. En el enlace de las dos estaciones participantes una es maestra y la otra la esclava, donde la responsabilidad del enlace recae sobre la maestra ya que todas las transmisiones van a o desde ella.
En la capa de red se ha definido el protocolo IrLMP (Infrared Link Management Protocol) el cual se encarga del seguimiento de los servicios como una impresión, así como de los recursos disponibles.
En la capa de transporte se define el protocolo IRTP (Infrared Transport Protocol) que se encarga de permitir que un dispositivo establezca multiples haces de datos en un solo enlace, cada uno con su propio flujo de control es decir permite la multiplexación de los datos.

- **Tecnología de radiofrecuencia.**

Las características de la capa física y subcapa MAC para la radiofrecuencia son:

- Frecuencia de trabajo: 2.4 GHz para los sistemas que se basan en el espectro disperso con un ancho de banda de 83 MHz.
- Velocidad de transmisión: 1 ó 2 Mbps.
- Modo de transmisión: Salto de frecuencia o Secuencia directa.
  - Salto de frecuencia. Emplea la modulación GFSK (Gaussian Frequency Shift Keying) de 2 o 4 niveles para 1 Mbps (2 Mbps opcional). La banda ancha se divide en 79 bandas de 1 MHz. Cada banda esta sujeta a un mínimo de 2.5 saltos por segundo usando uno cualquiera de tres esquemas posibles. Esto asegura que cada paquete enviado puede transmitirse en un solo salto de manera que la información destruida puede recuperarse en otro salto.
  - Secuencia directa. 1 Mbps con una modulación DBPSK (Differential Binary Phase Shift Keying) y 2 Mbps con DQPSK (Differential Quadrature Phase Shift Keying). Utiliza 5 sub-bandas de 26 Mhz centradas en las frecuencias 2.412, 2.427, 2.442, 2.457 y 2.40 GHZ.

Se puede aumentar la velocidad de transmisión de datos usando otras técnicas de modulación como:

- MBOK (Mary Bi-Orthogonal Keying) que permite conseguir tasas de datos de 5.5. y 11 Mbps (si la velocidad de transmisión es de 1 o 2 Megabaudios), el problema con esta técnica es su falta de compatibilidad con todos los productos 802.11.
- CCK (Complementary Code Keying) permite conseguir tasas de datos de 5.5 y 11 Mbps (dependiendo si la velocidad de transmisión es de 1 o 2 Megabaudios) y es totalmente compatible con todos los productos 802.11.

2.5.6 Elementos de una red Lan

Las redes de computadoras se constituyen de un conjunto de componentes de uso común y que en mayor o menor medida siempre aparecerán en cualquier red LAN instalada. Este conjunto de componentes se divide en dos grandes grupos: el hardware y el software. De entre la gran variedad de elementos que hoy en día constituyen una red podríamos mencionar que los principales son: las tarjetas de interfaz de red, cableado, protocolos de comunicaciones, sistemas operativos de red, aplicaciones capaces de funcionar en red y los elementos de conectividad.

2.5.6.1 Hardware

El hardware es el conjunto de elementos físicos que se pueden interconectar entre sí dentro de una red.

Tarjetas de red

Dentro del hardware de red existe un elemento muy importante que es el pilar de las redes locales y elemento imprescindible para instalar la red más básica, es decir, conectar dos estaciones, este elemento es la tarjeta de interfaz de red NIC (Network Interface Card). Las tarjetas de red son los adaptadores que se instalan en los dispositivos y en el caso de las estaciones de trabajo se insertan como cualquier otra tarjeta, para que estos se puedan conectar físicamente a la red.

Su función principal es proporcionar el puerto de interfaz físico adecuado para enviar y recibir la señal de comunicación desde y hacia el medio y procesarla para adaptar la información a transmitir o detectar. La interfaz de red tiene dentro de su circuiteria el código o algoritmo del protocolo físico de la red y que es dependiente de la tecnología que se este usando.

Todos los accesos a la red se realizan a través de las tarjetas de red por lo que deben ser tarjetas rápidas si se quieren obtener comunicaciones fluidas.

Existen tarjetas para distintos tipos de redes, las tarjetas más populares son las tarjetas ethernet, aunque también existen conectores LocalTalk, así como tarjetas TokenRing.

Sus características son:

- Operan en el nivel físico del modelo OSI, en este nivel se definen sus características mecánicas (como los conectores para el cable), sus características eléctricas (definición de los métodos de transmisión de la información y las señales de control para realizar dicha transferencia), el método de acceso al medio (algoritmo que se usara para acceder al medio que sostiene la red). Los métodos de acceso se definen por las normas IEEE802.x.
- Los circuitos de la tarjeta determinan antes de transmitir la información ciertos parámetros como la velocidad de transmisión, tamaño del paquete, timeout, tamaño de los buffers, etc. En el momento que estos parámetros se establecen inicia la transmisión, para lo cual convierte los datos de paralelo a serie para ser transmitidos como un flujo de bits, después codifica los datos y si es necesario se les aplica una compresión para mejorar el rendimiento de la transmisión.

- La tarjeta de red tiene una dirección física asignada que depende de los protocolos de comunicación que este utilizando. Esta dirección es definida desde la fabricación. Sobre esta dirección física se definen otras direcciones como la dirección IP.

2.5.6.1.1 Servidores

Los servidores conforman el corazón de la mayoría de las redes. Son equipos con mucha memoria RAM, un disco duro de gran capacidad y una tarjeta de red de alta velocidad y un procesador poderoso, estas características le dan a los servidores la capacidad de guardar grandes cantidades de información y la capacidad de compartir esta misma información, de forma rápida y eficiente. La función de los servidores es compartir sus recursos físicos y/o lógicos, la información y ejecutar el software servidor.
En los sistemas centralizados estos equipos ejecutan el sistema operativo de red, y soportan los recursos compartidos: unidades de disco, compartición de archivos, el software de impresión, trazadores, bases de datos así como otras aplicaciones compartidas. Por ejemplo un servidor de impresión se encargara de controlar gran parte del tráfico de red ya que él atenderá las peticiones de las estaciones de trabajo proporcionándoles los servicios solicitados de impresión.
En este punto es bueno aclarar que el concepto de servidor no debe verse como si existiera un equipo dedicado para cada función, esto es, un equipo servidor de archivos, un equipo servidor de impresión, etc. Lo adecuado es considerar a los servidores como procesos que proporcionan servicios en lugar de equipos específicos. Esta es una concepción mas apropiada de un servidor ya que muchos de ellos se implementan en paquetes de software capaces de funcionar en cualquier plataforma de hardware.
Los servidores pueden ser muchos y muy variados de entre los cuales destacan:

- Servidor de impresión.
- Servidor de disco.
- Servidor de ficheros o Base de datos.
- Servidor de terminales.
- Servidor de comunicaciones.
- Servidor de ejecución remota.
- Servidor de nombres.
- Servidor de transacciones.
- Servidor de aplicaciones.

Servidor de impresión
El servidor de impresión gestiona el acceso de los usuarios y el uso de las impresoras de distinto tipo (matriciales, láser, inyección de tinta, burbuja, etc.) y controla el acceso a las mismas. Su funcionamiento es de la siguiente forma: la información a imprimir es recibida por el software del sistema, esta información puede venir de una computadora o de otro servidor por ejemplo un servidor de archivos, el software del sistema transfiere la información al servidor de impresión en un formato comprensible por la impresora. El servidor de impresión imprime el trabajo o si ya tiene otros trabajos en curso encola las peticiones de impresión que le van llegando en su área de almacenamiento (spooler). Los

trabajos se imprimen en el mismo orden con el que llegan, aunque se puede cambiar la prioridad.

Servidor de disco

La función principal de este servidor es proporcionar a los usuarios de la red gran cantidad de almacenamiento secundario sin modificar la información. Este almacenamiento que proporciona son bloques de disco que los usuarios pueden leer y escribir. Para esto en el disco del servidor se realizan particiones del mismo y cada partición se asigna a los usuarios que trabajan en ellas guardando y leyendo información como si fuera su propio disco. Algunas de esas particiones son publicas por lo que cualquiera puede acceder a su información pero no la puede modificar, es decir son de solo lectura.

Estos servidores además de permitir la compartición de información reducen costos ya que así las estaciones pueden instalarse sin disco. Esto además incrementa la seguridad informática, pues existe información critica que no puede estar en cualquier computadora, por lo que se puede tener disponible en este tipo de servidor y con restricciones para los usuarios autorizados.

Servidor de archivos

Los servidores de archivo son programas que permiten el acceso a disco o cualquier otro dispositivo de almacenamiento de forma mas sofisticada que los servidores de disco. El servidor de archivos permite gestionar el acceso a los datos con distintos tamaños. Estos servidores pueden ser del tipo secuencial, de acceso directo indexado pero por ser su interfaz muy básica se complementan con algún otro componente como:

- Sistema de archivos que proporciona los mecanismos de protección, estructura de directorios, etc.
- Servidor de bases de datos, con el que se ofrece una gestión de transacciones complejas en entornos multiusuario, diferentes lenguajes y utilidades para definir, manipular y controlar datos, etc.
- Sistemas de memoria virtual que permiten que las estaciones que no tiene disco empleen la memoria del servidor como extensión de su memoria principal.

El servidor de archivos puede ser usado para el almacenamiento de archivos y de datos.

Servidor de terminales

Estos servidores también se conocen como concentradores ya que permiten conectar terminales ASCII o impresoras a la red local. Así cuando se quiere conectar una terminal al computador central por medio de una red de área local, el servidor de terminales recoge la entrada del terminal y la encapsula en una trama de red para transmitirla a su destino.

Servidor de comunicaciones

Los servidores de comunicaciones permiten conectar una red de área local a una red conmutada, a una red dedicada o a una red de paquetes. En el otro extremo de la conexión se puede encontrar una estación de trabajo, otra red local o un computador central. El servidor de comunicaciones gestionara el flujo de datos y mensajes de correo electrónico entre las propias redes de los servidores y otras redes o usuarios remotos que se conectan a los servidores usando módems y líneas telefónicas.

Servidores de ejecución remota
Estos servidores permiten que un programa particular se ejecute en otro computador diferente al que estamos utilizando. Así por ejemplo la mayor parte del trabajo se puede realizar en una computadora pequeña pero existen tareas que para ejecutarse necesitan los recursos del sistema.

Servidores de nombres
En sistemas muy grandes hay una gran cantidad de nombres de usuarios, contraseñas, direcciones de red, etc., que hacen muy difícil y tediosa su gestión. En estos casos los servidores de nombre son de gran utilidad facilitando el almacenamiento y actualización de estos elementos.

Servidores de transacciones
Son el soporte para la realización o ejecución de procesos transaccionales. Por ejemplo en negocios donde se acepta el pago con tarjetas de crédito al momento de pasar dicha tarjeta por el punto de venta esta puede mandar la solicitud de autorización a un servidor, entonces este realizara y controlara la autorización directamente con el banco.

Servidores de aplicaciones
Los servidores de aplicaciones son el lado servidor de las aplicaciones cliente/servidor, así como los datos disponibles para los clientes. Estos servidores almacenan grandes cantidades de datos organizados para facilitar su recuperación. Su base de datos no se carga a memoria de la terminal que la consulta sino que permanece en el servidor y solo se envían los resultados de la consulta. Como ejemplo tenemos a los servidores de correo, estos son aplicaciones servidor y cliente por separado, donde los datos son descargados de forma selectiva del servidor al cliente.

Servidores de servicios de directorio
Estos servidores permiten a los usuarios localizar, almacenar y proteger información en la red. Por ejemplo el software combinara los equipos en dominios que permiten que cualquier usuario de la red tenga acceso a cualquier recurso de la misma.

2.5.6.1.2 Estaciones de trabajo

Las estaciones de trabajo son los equipos de cómputo con los cuales los usuarios de la red realizan su trabajo cotidiano como redactar documentos, enviar correos, trabajos de diseño grafico, etc., estos equipos en un sistema centralizado se conectan al servidor. No son tan potentes como el servidor, mediante la tarjeta de red, el cableado pertinente y el software necesario se comunican con el servidor, pueden carecer de disquetera y disco duro y trabajar directamente sobre el servidor.
En una arquitectura cliente-servidor cualquier computadora puede trabajar como servidor y cliente a la vez.

2.5.6.1.3 Periféricos

Los periféricos son dispositivos que se pueden integrar a la red y que tienen funciones particulares y especificas como son las impresoras, plotters, escáneres, torres de CD, unidades de respaldo, faxes, módems, etc.

2.5.6.1.4 Medios de comunicación

Los medios de comunicación son el canal físico o no físico por el cual se transmite la información en las redes. Se constituye básicamente con el sistema de cableado utilizado para conectar los componentes de la red. El cable puede ser coaxial, par trenzado o fibra óptica para el caso de las redes de área local cableadas, para el caso de las redes inalámbricas son los rayos infrarrojos y las ondas de radiofrecuencia.[1].

En este punto no se puede dejar pasar como un elemento importante de las redes LAN el sistema de cableado estructurado, el cual es el que sostiene a los medios de comunicación.

El sistema de cableado estructurado es un sistema de administración centralizado y soporte de la infraestructura de comunicaciones ya sea voz, datos, textos, imágenes, etc. Se llama estructurado por que obedece a una estructura definida.

El sistema se compone de subsistemas:

- Horizontal. Este subsistema es el conjunto de medios de transmisión como cables, coaxiales, fibras ópticas que unen los puntos de distribución de planta con el conector o conectores del puesto de trabajo instalados previamente mediante un proyecto de ingeniería.
- Vertical. El subsistema vertical se compone del conjunto de cables que interconectan las diferentes plantas y zonas entre los puntos de distribución y administración.
- Administración principal. Es el punto de distribución principal del edificio en cuestión que normalmente se ubica en el sótano o planta baja y es a donde llega el cable de la red publica y donde se instalan los equipos como servidores y conmutadores.
- Administración de planta. Se compone de pequeños distribuidores que se ubican por las distintas plantas del edificio.

El sistema de cableado estructurado permite acabar con las anteriores infraestructuras de voz y datos principalmente separadas y algunos problemas como:

- Convivencia de cables de diferentes tipos: telefónico, coaxial, pares sin apantallar con diferentes numero de conductores, etc.
- Etiquetado del cableado inexistente, por lo que su reutilización para alguna nueva función es imposible.
- Imposibilidad de aprovechar el mismo tipo de cable para diferentes equipos.
- Peligro de interferencias, averías y daños personales al mezclar cables de transmisión con los de suministro eléctrico.
- Coexistencia de diferentes tipos de conectores.
- Diferentes topologías de cableado, estrella, bus, anillo.
- Posibles accidentes provocados por el acumulamiento y desorden del cableado en techos falsos.

[1] El tema de medios de comunicación se vio en el tema 2.5.3.1 Medios de transmisión de redes LAN

- Generación de costos de materiales, mano de obra, horas-hombre perdidas y recableado para la reubicación de un equipo informatico o telefónico.
- Dificultad para el mantenimiento y acceso de los cables.

Las ventajas del sistema de cableado estructurado son:

- Trazados homogéneos.
- Reubicación más sencilla, barata y eficiente de equipos.
- Convivencia de distintos sistemas sobre el mismo soporte físico.
- Transmisión a altas velocidades para redes.
- Mantenimiento mucho más rápido y sencillo.

2.5.6.1.5 Elementos de conectividad

Los dispositivos de conectividad tienen la funcional primordial de recibir y reenviar la información que los medios de comunicación transmiten.

No basta con tener las computadoras en una sala conectadas es necesario conectarlas a su vez con las computadoras del resto de las salas de una empresa y con el resto de las sucursales de una empresa situadas en distintos puntos geográficos. La interconexión de redes aunque permite ampliar el tamaño de una intranet se utiliza también para conectar redes independientes.

El numero de computadoras que componen una red esta limitado por la topología, aunque si se quisiera sobrepasar el número de computadoras conectadas se podría pensar en segmentar la intranet. Al elegir la topología de una red se deben tomar en cuenta factores como la densidad de trafico que debe soportar, el tipo de aplicaciones que van a correr sobre la red, la forma de trabajo que debe gestionar, entre otras. En una misma empresa se puede tener no solamente una sola intranet aunque sea segmentada, si no también se pueden tener redes independientes, con topologías diferentes e incluso arquitecturas diferentes y que estén interconectadas. Por lo tanto pueden encontrarse dentro de un mismo edificio varias intranets con diferentes topologías y con el tiempo puede surgir la necesidad de interconectarlas. Por estas y otras razones se hace necesaria tanto la segmentación como la interconexión de intranets.

En la tabla 2.5.6.1.5.1 se presentan algunos casos en los que se tiene necesidad de segmentar y/o interconectar intranets.

Necesidad	Solución
Con el manejo de aplicaciones que producen un aumento importante del trafico en la red se baja el rendimiento de la misma	Dividir la red actual en varios segmentos: segmentar la red.
Se quiere ampliar el numero de nodos que forman la intranet pero se quiere mantener el rendimiento de la red	Crear un nuevo segmento de red para los nuevos nodos e incluso se pueden mover nodos que por su ubicación es más conveniente que pertenezcan al nuevo segmento
Se quiere unir dos intranets exactamente iguales en la empresa.	Se pueden interconectar con un dispositivo de bajo nivel o bien definir una de ellas como un segmento de la otra y unirlas
Se necesita unir dos o más redes con diferentes topologías pero trabajando con los mismos protocolos de comunicaciones	Se pueden interconectar ambas redes con dispositivos de nivel medio
Se necesita conectar dos o más redes totalmente diferentes, es decir de arquitecturas diferentes	Se pueden interconectar ambas redes a través de dispositivos de alto nivel.

Tabla 2.5.6.1.5.1 Casos de segmentación.

Segmento

Un segmento es un bus lineal al que se conectan varias computadoras y que termina en los extremos. Sus caracteririticas son:

- Cuando se tiene una red grande se divide en trozos, llamando segmentos a cada uno de ellos.
- Para interconectar varios segmentos se utilizan puentes (bridges) o ruteadores (routers).
- El rendimiento de una red aumenta al dividirla en segmentos.
- A cada segmento y a las computadoras conectadas a él se le llama subred.

Par implementar la segmentación se crean subredes pequeñas con lo que se aumenta el numero de computadoras conectadas a la red y se mantiene su rendimiento. debido a que en la misma intranet se producen varias comunicaciones de forma simultanea. Las propias subredes se gestionaran para permitir la comunicación entre segmentos cuando sea necesario. Los segmentos están restringidos a ciertas longitudes dependiendo de las topologías de red como se observa en la tabla 2.5.6.1.5.2

Topología	Longitud
Ethernet gruesa	500 metros
Ethernet fina	185 metros
Ethernet de par trenzado	100 metros
Ethernet de fibra óptica	2000 metros
Token-Ring de par trenzado	100 metros

Tabla 2.5.6.1.5.2 Tabla de longitudes de los segmentos de red.

El dispositivo usado para segmentar una red debe ser capaz de decidir hacia que segmento debe enviar la información, debe decidir si la envía al mismo segmento de donde proviene la información o a otro diferente.
Los motivos que hacen necesaria la segmentación de una red pueden ser:

- Limitaciones en el numero de hosts
- Limitaciones en el número y tipo de nodos por lo que se hace necesario aumentar el número de nodos que la topología permite. La limitación del número de nodos se puede dar debido al método de acceso al medio, por el tipo de cable, por el ancho de banda, etc.
- Limitaciones en la distancia que se puede cubrir.
- Limitaciones en el acceso a los nodos y la comunicación con los usuarios por lo que se requiere mejorar el rendimiento de una red en la que se ha aumentado el tráfico. Una intranet que inicialmente funciona bien con un tiempo de respuesta aceptable, empieza a perder prestaciones cuando se incrementa el numero de comunicaciones que la red gestiona debido al crecimiento de nodos y a que los usuarios aprovechan mas la red instalando mas aplicaciones.

Para solucionar estos problemas se pueden hacer desde cambios físicos drásticos como la sustitución del cable por otro que soporte mayores velocidades, cambiar las tarjetas de red por otras más rápidas e incluso cambiar la topología de la red. Pero para evitar estos cambios muchas veces innecesarios se hace la segmentación de la red por áreas, aulas o departamentos con una subred por departamento con lo cual en cada departamento se mejorara el rendimiento de la red. Esta interconexión de intranets o subredes o la segmentación se puede establecer a varios niveles desde el nivel físico hasta niveles más altos del modelo OSI. La tabla 2.5.6.1.5.3 muestra el nivel en que trabajan los diferentes dispositivos de conectividad de una red LAN.

Dispositivo	Nivel
Concentrador	Físico
Repetidor	Físico
Puente	Enlace
Ruteador	Red
Pasarela	Aplicación

Tabla 2.5.6.1.5.3 Dispositivos de interconexión de red y nivel de funcionamiento

2.5.6.1.5.1 Hubs

Un hub también llamado concentrador o repetidor multipuerto es un elemento que trabaja en la capa 1 (física) del modelo OSI. Fig. 2.5.6.1.5.1.1.

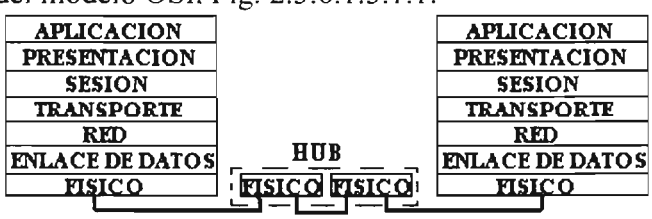


Fig. 2.5.6.1.5.1.1 Nivel de funcionamiento de un HUB

El hub proporciona una conexión central para todos los cables de la red, en esta conexión central se unen los hosts dentro de una red. Es el dispositivo de interconexión de hosts más simple que existe y actualmente ya no es muy usado. Físicamente estos equipos son cajas con un numero determinado de puertos en los que se insertan los conectores de los cables de red para conectar de esta manera a los dispositivos en red, normalmente los conectores son RJ45.

El hub recibe la señal por un puerto y la reproduce por todos los demás puertos. Los primeros hubs eran meros concentradores/repetidores que permitían la conexión de los dispositivos a la red. Los hub llamados multimedia tenían un conector adicional de tipo diferente para conectar otro tipo de red o medio físico diferente. También se proveen con salidas especiales para conectar otro hub permitiendo así ampliaciones de la red. Sus principales características son:

- La caja es un armario de conexiones donde se centralizan todas las conexiones de una red. Físicamente es un dispositivo con muchos puertos de entrada y salida.
- Se utilizan para conectar dos o más segmentos ethernet de cualquier tipo de medio.
- No tiene ninguna función aparte de centralizar conexiones.
- Se pueden utilizar para implementar topologías en estrella física pero pueden funcionar como un anillo o bus lógico.
- Algunos pueden repetir y amplificar la señal permitiendo conectar nodos a distancias mayores que los más simples.
- Proporciona la ventaja de concentrar a los usuarios facilitando las tareas de administración y diseño de la red.
- Los hubs al trabajar en un medio compartido donde todos los dispositivos están conectados a él, tiene problemas de congestión de la red debido a las tormentas (broadcast) de información que pueden llegar a ocurrir por la información que transmite un dispositivo hacia todos los demás al mismo tiempo, si a esto le agregamos que el segmento este sobreocupado se incrementa el numero de colisiones. Por lo tanto en un sistema de red con hub tenemos un solo dominio de colisiones y un dominio de broadcast, como muestra la Fig. 2.5.6.1.5.1.2

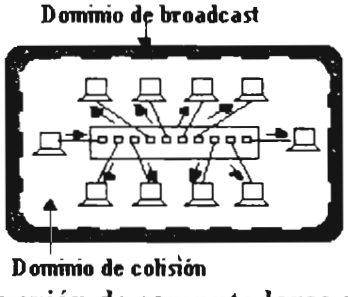


Fig. 2.5.6.1.5.1.2 Conexión de computadoras en red mediante hub

Como se puede observar en la Fig. 2.5.6.1.5.1.2, se tiene un solo dominio de broadcast, el dominio de broadcast es el conjunto de segmentos por donde una trama de broadcast (dirección de difusión que manda un mensaje a todas las direcciones físicas MAC FF-FF-FF-FF-FF-FF) se debe propagar, debido a que en un hub las tramas que llegan por una

interfase se propagan a todos los puertos, el dominio de broadcast es uno solo ya que el hub forma un solo segmento. Por lo que una trama de broadcast llegara a todos los equipos conectados al hub.
Asimismo el dominio de colisiones es uno solo, el dominio de colisiones es el segmento o tramo de medio físico por donde circulan las tramas que forman el tráfico originado en las interfaces, igual que en el dominio de broadcast el tráfico originado en una interfaz circula por todas las demás interfaces.

2.5.6.1.5.2 Repetidores

Debido a que las señales pierden fuerza o se atenúan a medida que avanzan a lo largo de un cable que conecta a dos hosts cuya distancia es grande, esa pérdida de señal puede provocar que haya pérdida de información. El repetidor amplifica y regenera la señal entre los dos segmentos que interconecta, compensando la atenuación y distorsión debidas a la propagación por el medio físico. Los repetidores trabajan a nivel físico, Fig. 2.5.6.1.5.2.1, solo actúan sobre los bits transferidos entre los niveles físicos de dos estaciones, por lo tanto son transparentes al subnivel MAC y niveles superiores.

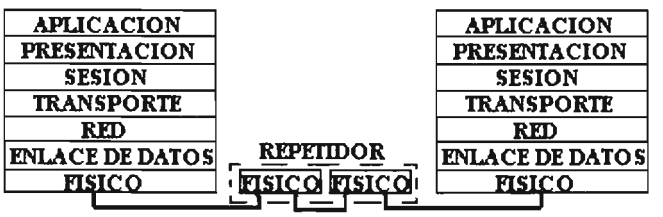


Fig. 2.5.6.1.5.2.1 Nivel de trabajo del repetidor

Como trabajan a nivel físico no verifican errores, rutas de paquetes ni poseen dominios de colisión. Su funcionamiento es el siguiente: toman la señal que circula por la red la amplifican, la reproducen fielmente y la propagan nuevamente sin efectuar ningún tipo de interpretación o traducción de la señal, de esta manera permiten que la distancia entre dos puntos de la red sea mayor que la que un solo cable permite.
Si los enlaces difieren en algún sentido (topología o método de acceso) se requiere un dispositivo más complejo. Los repetidores pueden conectar diferentes medios de transmisión, ya que esto solo requiere cambiar el formato físico de las señales, pero por ejemplo no pueden conectar redes de banda base con redes de banda ancha ya que los métodos de decodificación son diferentes y son operaciones más complejas.
En general los repetidores son dispositivos de uso limitado que se emplean para interconectar redes locales homogéneas.
Sus características son:

- Conecta a nivel físico dos intranets o dos segmentos de intranet.
- Permite resolver problemas de limitación de distancias en un segmento de intranet repitiendo la señal transmitida para cancelar la atenuación, de esta forma se incrementa la longitud del cable que soporta la red.
- Operan con cualquier tipo de protocolo, ya que solo trabajan con señales físicas.
- Al trabajar al nivel mas bajo de la pila de protocolos obliga a que:

- Los dos segmentos que interconecta tengan el mismo acceso al medio y trabajen con los mismos protocolos.
- Los dos segmentos tengan la misma dirección de red.

• Debido a que no procesan tramas su efecto sobre el retardo de propagación de la señal es mínimo ya que no existe ningún software ni interfaz entre niveles en su modo de operación.
• Son baratos debido a su simplicidad.
• Se utilizan tanto en redes de área local como en redes de área extensa.

2.5.6.1.5.3 Bridges

Los puentes o bridges son dispositivos que trabajan en la capa 2, Fig. 2.5.6.1.5.3.1, por lo que operan sobre las tramas que se transfieren en los niveles de enlace de datos, particularmente sobre el nivel de acceso al medio MAC.

Fig. 2.5.6.1.5.3.1 Nivel de operación de los puentes

Los puentes conectan dos o más redes LAN que utilizan los mismos protocolos, aunque las topologías de red sean diferentes como Ethernet y Token Ring. Además filtran el tráfico de la red a nivel básico.
El puente debe accesar a cada uno de los enlaces físicos de acuerdo a los métodos de acceso de cada red, debido a esto el acceso no es inmediato, por lo que debe tener la capacidad de almacenar y posteriormente reenviar las tramas (store and forward). Esta capacidad de almacenamiento y reenvío le permite examinar los campos de dirección (física) de las tramas (para realizar un filtrado) para reenviarlas basándose en el conocimiento de la red donde se localiza el nodo destino. Si la dirección origen no esta en su tabla de destinos, la agrega junto con un indicador de la red local a la que pertenece. Mediante una función de autoaprendizaje (self learning task bridges) estos equipos determinan la dirección ethernet del usuario en el segmento construyendo una tabla a medida que los paquetes pasan a través de él, con esta característica se pueden añadir estaciones en cualquiera de las redes sin necesidad de actualizar la tabla de destinos en forma manual.
Con base en la característica de identificar la dirección física dentro de los paquetes que entran y salen a través de sus puertos y la construcción de la tabla de asociación Dirección/Puerto, pueden tomar decisiones para segmentar el tráfico de redes grandes en redes más pequeñas, Fig. 2.5.6.1.5.3.2. Son usados para conectar varias LAN (iguales o distintas) para separar el trafico entre estas o por si usan tecnologías diferentes. Esta segmentación deja salir el tráfico de una red que va destinado a otra red, mientras que todo el tráfico interno seguirá en la misma red. Con esto se consigue una reducción del tráfico de la red.

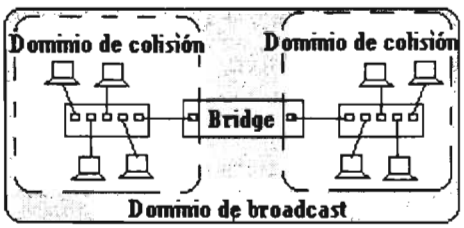


Fig. 2.5.6.1.5.3.2 Segmentación de una red mediante un bridge

En la Fig. 2.5.6.1.5.3.2. vemos que al filtrar las direcciones y rechazar los paquetes que van al mismo segmento de la interfaz por la que llegaron se forma un dominio de colisión en cada red que se conecta, con lo que una red no será afectada por las colisiones en la otra.
El puente normalmente conecta LANs con idénticos protocolos de capa física y de acceso al medio (MAC), ya que estos dispositivos trabajan en la subcapa de acceso al medio sin añadir ninguna información adicional a la trama, las razones para conectar varias LAN (segmentar) son las siguientes:

- Al conectar varias LAN con puentes, cuando falla una LAN no afecta a la(s) otra(s).
- Varias LAN pequeñas tienen mejores prestaciones que una grande, sobre todo por que las longitudes de cableado son menores.
- El filtrado de paquetes y la regeneración de paquetes enviados permite a la tecnología de bridging partir una red en dominios de colisión separados.
- Se puede implementar una seguridad básica al conectar la LAN de un área segura por medio de un puente a las otras para que no se vea el tráfico interno del área segura.

Las funciones y características de un puente son:

- El puente capta las tramas de una LAN con un protocolo MAC, las emite en la otra LAN que tiene el mismo protocolo MAC por lo cual no modifica las tramas.
- Autoaprendizaje, filtrado y reenvió. El puente determina los segmentos origen y destino de un paquete, para esto debe conocer el suficiente direccionamiento o si no agregar las direcciones (autoaprendizaje) para saber encaminar (reenvío) las tramas que van a una LAN y las que van a la otra dejando pasar solo el trafico necesario, esto cuando se conectan mas de dos LAN, cuando se tienen dos LAN únicamente se realiza una retransmisión. El encaminamiento (filtrado) puede hacerse estáticamente o con tablas de encaminamiento actualizadas automáticamente. Cuando el paquete que le llega tiene como destino el mismo segmento por el que entro, el bridge no lo transmite simplemente lo descarta (dropped o filtered) si los segmentos son distintos entonces el paquete es transferido al segmento correcto.
- Resuelve el problema de limitación de distancias junto con el problema de limitación del número de nodos de una red.
- Trabajan en nivel de enlace del modelo OSI por lo que pueden interconectar redes que cumplan las normas del modelo 802 (3, 4 y 5). Operan transparentemente al nivel de red y superiores, si los protocolos por encima del nivel de enlace son diferentes en ambas redes y el puente no es consciente de ello, no puede resolver los problemas que puedan presentársele.
- No hay un límite conceptual para el número de puentes en una red.
- Evitan que paquetes dañados se distribuyan innecesariamente, por que no los retransmite.

- Cada segmento de red interconectada con un puente tiene una dirección de red diferente.
- Los puentes no entienden de direcciones lógicas ya que trabajan en otro nivel.
- Se usan en redes de área local, para:
- Extender la red, o ampliar el número de nodos que la constituyen.
- Reducir la carga en una red con mucho tráfico, uniendo los segmentos de esa red.
- Unir redes con la misma topología y método de acceso al medio o diferentes.
- Cuando une redes exactamente iguales su función se reduce exclusivamente a direccionar el paquete hacia la subred destino y segmentar el dominio de colisiones.
- Cuando une redes diferentes debe realizar funciones de traducción entre las tramas de una topología a otra.
- Los puentes realizan las siguientes funciones:
- Reenvío de tramas a modo de filtrado. Un puente solo reenvía a un segmento aquellos paquetes cuya dirección de red lo requiera, los paquetes que van dirigidos a nodos locales del mismo segmento no traspasan el puente, esto es, aísla trafico entre segmentos de red. Por lo tanto cuando un paquete llega a un puente este examina la dirección física destino contenida en el paquete, para determinar si el paquete debe atravesar el puente o no.
- Técnicas de aprendizaje. Los puentes construyen tablas de dirección que describen las rutas, ya sea mediante el examen de flujo de los paquetes (puenteado transparente) o bien con la obtención de la información de los paquetes exploradores (encaminamiento fuente) que han aprendido durante sus viajes la topología de la red. Los primeros puentes requerían que los administradores introdujeran manualmente las tablas de dirección.
- Los puentes trabajan con direcciones físicas. Por lo tanto pueden filtrar tramas por dirección física y por protocolo.

Los puentes son elementos de red que interconectan redes aislando el trafico de una y otra mediante la función de filtrado, pudiendo de esta forma incrementar el numero de nodos soportados así como el área cubierta. Un puente al tener mayor funcionalidad que un repetidor y dado que realiza una manipulación de la información, es decir procesa las tramas, introduce más retardo en la propagación de la señal.

2.5.6.1.5.4 Switches (Conmutadores)

Los switches o puentes multipuerto son dispositivos que trabajan en la capa 2 del modelo OSI, Fig. 2.5.6.1.5.4.1 y existen otros que trabajan en la capa 3, su objetivo principal es filtrar el trafico a nivel de direccionamiento físico MAC, para transmitir la información mas eficientemente.

Fig. 2.5.6.1.5.4.1 Nivel de funcionamiento de un switch

Estos dispositivos resuelven problemas de sobresuscripción de ancho de banda segmentando la red, ya que reduce el número de dispositivos contendiendo por acceder al medio de red con lo cual disminuye la carga de trafico en el segmento original. El switch establece dominios de colisión separados entre segmentos conectados, Fig. 2.5.6.1.5.4.2.

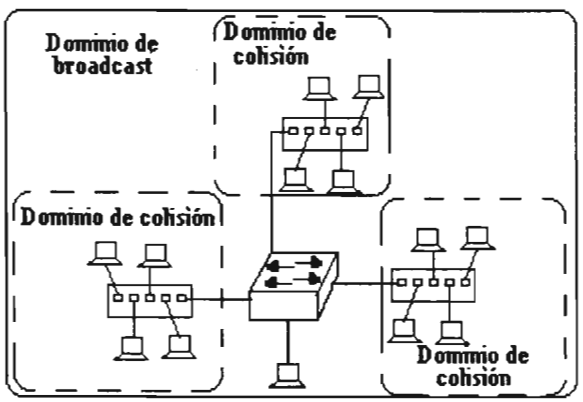


Fig. 2.5.6.1.5.4.2. Segmentación de una red con el uso de un switch.

Su principio de operación esta basado en una matriz de conmutación, maneja una tabla SAT (Source Address Table) similar a la de un bridge, cuando recibe un paquete por un puerto, el switch determina de la tabla de direcciones físicas el destino del paquete y establece una conexión dedicada por unos instantes de segundo entre las dos entidades que quieren comunicarse, esto ocurre de manera simultanea y muchos miles de veces por segundo. En comparación a un hub o router, el switch es más rápido que ambos. Es más rápido que el router por que trabaja en capa 2 del Modelo OSI, esto es, establece una comunicación de dirección física MAC a dirección física MAC, por esto no tiene que ejecutar todo un algoritmo como el router. Por otra parte es más rápido que el hub por que este ultimo hace broadcast lo que provoca que la red se inunde de la misma información.
Los switches tienen dos arquitecturas básicas: cut-through y store-and-forward.

- Los switches cut-through eran inicialmente los más rápidos ya que cuando un paquete ingresaba al switch este examinaba únicamente la dirección de destino antes de enviarlo al segmento de destino.
- Un switch store-and-forward analiza el paquete entero antes de enviarlo a su destino. Le toma mas tiempo examinar el paquete entero, pero le permite determinar posibles errores o daños en los paquetes y detener su propagación a través de la red. Actualmente la diferencia de velocidades entre ambos es casi igual.

Ambos switches separan la red en dominios de colisión, permitiendo extender las reglas de diseño de redes.

- Cada uno de los segmentos conectados a un switch ethernet posee un ancho de banda completo de 10 Mbps compartido por menos usuarios, lo cual permite un mejor desempeño, en contraposición a los hubs que solamente permiten compartir el ancho de banda en una Ethernet única.
- Una red compuesta de un numero de switches vinculados entre sí forman una red de backbone.
- Los switches originaron el nacimiento de la conmutación (switching) en el ámbito de redes de área local lo que permitió mejorar el control y funcionamiento de la red, una forma de implementar esto es mediante la creación de redes de área local virtuales VLAN.

Una VLAN es un dominio de broadcast definido vía software. Este dominio de broadcast es el equivalente a un puerto de un ruteador. En redes TCP/IP una VLAN representa una subred de IP. Una VLAN se puede implementar en redes que requieran manejar más de un dominio de broadcast o donde se requiera segmentar la red. El mecanismo de VLAN examina y toma decisiones complejas a altas velocidades en ráfagas de paquetes por lo que deben implementarse a nivel de hardware con el mínimo soporte de software en tiempo real. Las ventajas de las VLAN son:

- Movilidad. Con las VLAN se pueden añadir usuarios a la red sin necesidad de reconfigurar las direcciones IP de cada estación, se puede configurar una VLAN en base a una política de dirección de red, en la cual se establece una subred a una VLAN (por ejemplo 192.0.254.x), entonces el usuario que se conecte a la red en cualquier punto físico si tiene una dirección IP perteneciente a esta subred pertenecerá a la VLAN.
- Soporte de múltiples tecnologías y rangos de conversión. A implementar una VLAN se pueden realizar conversiones entre tecnologías ethernet, ATM, Gigabit Ethernet, Token Ring, FDDI, etc.
- Seguridad y control. En las redes existen usuarios que trabajan con múltiples protocolos para diferentes aplicaciones. La VLAN se puede usar para proporcionar flexibilidad y control de acceso a las aplicaciones, para esto se puede establecer una VLAN que proporcione acceso únicamente a las aplicaciones internas y restringa el acceso a Internet.

LAS VLAN se pueden definir por puerto o por política, esta ultima es la más flexible y amigable. LAS VLAN por política se pueden definir de la siguiente forma:

- VLAN por puerto. Esta política permite integrar una lista de puertos a una VLAN.
- VLAN por direcciones MAC. En una VLAN se pueden agregar las direcciones MAC de los dispositivos que se desee pertenezcan al mismo dominio de broadcast.
- VLAN por protocolo. Se puede definir que los usuarios que usen el protocolo IP pertenezcan a una VLAN1 y los que usen IPX pertenezcan a la VLAN2.
- VLAN por subred. En una red TCP/IP una unidad básica de administración es la subred IP, la cual es un dominio de broadcast. Con las VLAN se pueden definir subredes dentro de una sola red, esto es muy útil para redes que cuenten con un gran numero de usuarios IP.
- VLAN por trafico multicast. Este tipo de VLAN permite definir un grupo de trabajo que recibe la misma distribución de trafico.

2.5.6.1.5.5 Routers

Los dispositivos ruteadores (routers o encaminadores) trabajan a nivel de red, Fig. 2.5.6.1.5.5.1, es decir operan sobre los paquetes transferidos entre los niveles de red de las estaciones.

Fig. 2.5.6.1.5.5.1 Nivel de operación del ruteador

Usan el nivel de red para dirigir el trafico de una red a otra, se podría decir que es un bridge con mas capacidades ya que además de incorporar la función de filtrado es capaz de leer la dirección lógica del paquete y calcular la ruta hacia el destino determinando cual será el camino mas rápido para llevar la información de un lugar a otro.
Los routers a diferencia de los switches y bridges que dividen la red físicamente, dividen la red lógicamente, pudiendo dividir la red en subredes de modo tal que solo el tráfico destinado a una dirección IP particular puede pasar a través de segmentos. Son capaces de enrutar paquetes por unos caminos más cortos que otros, así como buscar alternativas cuando un camino esta muy cargado, determinando cual es el camino más rápido y de menor costo.
Mientras un bridge conoce la dirección de las computadoras a cada uno de sus extremos, un router conoce la dirección tanto de las computadoras como de otros routers y bridges y es capaz de checar toda la red para encontrar el camino menos congestionado. La instalación de dispositivos de capa 2 en un ambiente de red para segmentar el trafico no elimina aun los problemas de sobresuscripción del medio de red, ya que controlan la cantidad de datos de usuario final sobre un segmento dado, pero al ser dispositivos de capa 2 no distinguen la propagación del trafico de broadcast entre segmentos. El trafico de broadcast de fuentes como el protocolo IPX para chateo de Novell o el proceso de resolución de nombres Netbios de Microsoft si no es confinado de buena forma podría monopolizar el ancho de banda de la red entera.
Aun con la segmentación de los switches existe una cantidad significativa de tráfico de broadcast que es transmitido entre segmentos de red. Una tormenta de broadcast puede deshabilitar la red completa.
El router no solo divide el dominio de colisión en segmentos separados, también divide el dominio de broadcast, manteniendo el trafico de broadcast local a cada segmento conectado, Fig. 2.5.6.1.5.5.2. Al reducir el broadcast propagado entre segmentos de LAN, la carga de tráfico completo de cada segmento decrece.

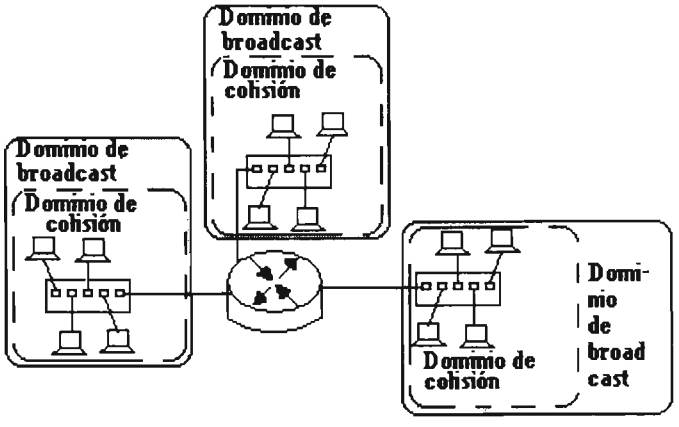


Fig. 2.5.6.1.5.5.2 División de los dominios de broadcast y de colisión por medio de un router.

Su funcionamiento es el siguiente:

- Cuando un paquete llega al router, este examina la dirección destino y lo envía a través de una ruta predeterminada.
- Si la dirección destino pertenece a una de las redes que el router interconecta entonces envía el paquete directamente a ella, en caso contrario enviara el paquete a otro router más próximo a la dirección destino.
- Para conocer el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento.

Sus principales características son:

- Por sus características avanzadas, trabajan a nivel de red del modelo OSI lo que les permite entender y manejar las direcciones lógicas (direcciones IP) de los paquetes.
- Almacenan información sobre las redes y rutas entre redes, incluyendo las redes que no se encuentran directamente conectadas entre sí, esto para transmitir los paquetes en la dirección mas adecuada siempre y cuando se trate de redes homogéneas que comparten el mismo protocolo de encaminamiento.
- Utilizan un esquema de direccionamiento jerárquico (tablas de rutas) que distingue entre la dirección de un dispositivo dentro de la red y la dirección de la red. Para esto deben incorporar protocolos de nivel de red y por lo tanto un router es independiente del protocolo de red.
- Los routers pueden ser estáticos o dinámicos según como manejen la información en sus tablas de ruteo. Cuando son estáticos, la actualización de sus tablas de ruteo se realiza por parte del administrador en forma manual. Cuando son dinámicos los protocolos de encaminamiento se encargan de la notificación automática de un cambio o avería mediante mensajes de difusión (broadcast) entre los encaminadores.
- Pueden interpretar los protocolos lógicos que la red este usando y en base a ello tomar decisiones sobre la ruta que debe llevar el paquete.
- Para poder realizar su función de encaminamiento los ruteadores deben emplear algún tipo de algoritmo el cual le permite calcular la distancia entre el router y la estación receptora del paquete, el número de saltos requeridos antes de llegar a ella, la capacidad de cada enlace o el tiempo de transferencia entre dos saltos

consecutivos. Un algoritmo básico muy empleado es el protocolo de información de encaminamiento RIP.
- Son capaces de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo.
- Permiten interconectar cualquier tipo de red: Paso de testigo, ethernet, x.25, etc.
- Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos, para ello incorporan un software que traduce o encapsula un protocolo en otro, aunque no son soportados todos los protocolos.
- Cada segmento de red conectado a través de un router tiene una dirección de red diferente, por lo que estos equipos permiten aislar totalmente segmentos de red convirtiéndolos en redes independientes o subredes.
- Permite conectar redes de área local y redes de área extensa. Generalmente están en la orilla de las redes LAN y funcionan como enlaces hacia otras redes LAN o hacia redes WAN.

Los ruteadores introducen mas retardo en el manejo de la información que los repetidores y puentes fundamentalmente por el tamaño de sus tablas, pero en contrapartida generan un menor tráfico de broadcast.
Existen algunos dispositivos con características de los puentes (transparencia a los protocolos con aprendizaje) y de los ruteadores (selección del camino óptimo), a estos dispositivos se les da el nombre de brouters (bridges y routers). El brouter funciona como encaminador cuando los protocolos de nivel superior permiten el encaminamiento. En caso contrario funcionan como puentes.

Estos son los dispositivos más comunes en las redes de datos aunque podríamos seguir comentando sobre otros dispositivos que por su uso tan común hoy en día se pueden considerar dentro de los elementos que componen una red de área local como por ejemplo los firewall que son equipos usados para proporcionar seguridad en la comunicación de las redes con otras redes externas, pero los comentados hasta aquí son los de uso más común.

2.5.6.2 Software

El software en su conjunto conforma los elementos de tipo lógico que hacen interactuar al hardware. Dentro de estos elementos de tipo lógico tenemos:
- Sistemas operativos de red.

Son el conjunto de programas que residen en el equipo central o servidor y que llevan a cabo la gestión de recursos físicos y lógicos de la red, es decir configura y reconoce al hardware y programas de aplicación. Además de incorporar las herramientas propias de un sistema operativo como el manejo de ficheros y directorios, incluyen otras para el uso, gestión y mantenimiento de la red, así como herramientas destinadas a correo electrónico, copia de ficheros entre nodos, ejecución de aplicaciones contenidas en otras maquinas, competición de recursos de hardware.
Comercialmente predominan en el mercado los sistemas operativos de Microsoft (Windows X), Novell, los diferentes sistemas operativos UNÍX, así como Solaris de Sun y LINUX, OS/2, etc. Cada sistema operativo ofrece una forma diferente de gestionar la red y utiliza diferentes protocolos para la comunicación. Estos sistemas operativos avanzados están diseñados para sacar el mejor provecho del hardware de los servidores mas avanzados.

El sistema operativo de red es el que soporta el intercambio de información a nivel software por lo que tiene que residir tanto en el cliente como en el servidor.

- Controlador/driver.

Es el programa que contiene las instrucciones necesarias para que un elemento de hardware sea reconocido y pueda interactuar con otro elemento de hardware y los sistemas operativos.

- Protocolo lógico.

Es el conjunto de normas que regulan la comunicación entre los elementos de software de la red. El protocolo lógico es dependiente del sistema operativo. Dentro de los protocolos lógicos podemos mencionar a TCP/IP, IPX/SPX, NetBIOS, NETBEUI, DECNet. APPLETALK etc.

- Software cliente.

Es el sistema operativo de red que reside en las estaciones de trabajo (clientes) y que permite la comunicación con el sistema operativo de la red.

- Aplicaciones.

Son todos los programas que el usuario utiliza directa o indirectamente para el procesamiento de la información. Este es el software de tipo front end, ya que es un software ligero que se ejecuta en las estaciones que no son equipos tan poderosos. Las aplicaciones que se ejecuten en servidores como bases de datos son de tipo back end ya que se necesita hardware robusto par su ejecución.

- Sistema de gestión de red.

Este sistema permite controlar las prestaciones, problemas, seguridad o configuración de la red.

- Gateways.

Son dispositivos que trabajan a nivel de presentación entre dos redes distintas. Sus características son:

- Se trata de un ordenador u otro dispositivo que interconecta redes radicalmente distintas.
- Trabaja al nivel de aplicación del modelo OSI.
- Cuando se habla de pasarelas en el ámbito de redes de área local, en realidad se esta hablando de routers.
- Son capaces de traducir información de una aplicación a otra como por ejemplo las pasarelas de correo electrónico.

Los gateways pueden ser implementaciones en hardware o software o un modelo combinado que proporcionan la conectividad física y lógica entre una red LAN y un sistema o red de diferente arquitectura como puede ser un enlace a un mainframe o una aplicación de salida a Internet.

2.5.7 Redes inalámbricas

Definición, características y funciones de una red inalámbrica (WLAN)

Una red de área local es la que cubre un entorno geográfico limitado con una velocidad de transferencia de datos relativamente alta (mayor o igual a 1 Mbps) con una tasa de errores baja y administrada de forma privada.
Las redes de área local inalámbricas son redes de alcance local que tienen como medio de transmisión el aire. Una red inalámbrica WLAN (Wireless Local Area Network) tiene las mismas características que la red LAN mas una adicional que la distingue de las redes LAN comunes o cableadas, utiliza ondas electromagnéticas como medio de transmisión de la información, la información viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Los enlaces inalámbricos se implementan básicamente con tecnologías de ondas de radio, microondas e infrarrojos.
Los medios existentes de comunicación como el UTP telefónico y cable coaxial para televisión siguen siendo los preferidos para establecer las conexiones de alta velocidad para acceso a redes de datos y a Internet. El problema con estos medios de comunicación es la dificultad de instalación en lugares distantes o que por sus características geográficas y topológicas no cuentan con una infraestructura de cableado o no es posible instalarla. De esto se despenden los atractivos de las redes WLAN que son fáciles de instalar y llegan a lugares de difícil acceso para el cableado.
Los sistemas de radiofrecuencia contribuyeron a desarrollar las comunicaciones de voz y datos a baja velocidad en este tipo de ambientes al igual que los sistemas satelitales, pero las tasas de transmisión son bajas debido a que los anchos de banda son limitados y requieren mucha verificación, lo que impide tener una comunicación eficaz.
Las primeras tecnologías inalámbricas operaban a una frecuencia de 900 Mhz y eran de baja velocidad, 1 o 2 Mbps, las ofertas tecnológicas eran propietarias, la libertad y flexibilidad de los sistemas inalámbricos les permitió abrirse camino en los mercados de comunicaciones LAN y otros mercados de recolección de datos.
En 1992 se inician las primeras investigaciones y desarrollo de productos operando a 2.4 Ghz. Ya que en la banda de 900 Mhz se tenían problemas con teléfonos celulares e inalámbricos.
Como la tecnología ethernet predomina en las redes alambricas y proporciona estándares abiertos e interoperables para fabricantes, usuarios de redes y comunicaciones se pensó en una base abierta y similar como cimiento de la tecnología inalámbrica.
La función principal de las redes inalámbricas es proporcionar conectividad y acceso a las tradicionales redes cableadas como una extensión de ellas pero con la flexibilidad y movilidad que les da las redes inalámbricas. De aquí que valga la pena aclarar que las tecnológicas inalámbricas no buscan sustituir a las redes cableadas sino complementarlas aportando las facilidades propias de los sistemas sin cables.
Las funciones o aplicaciones de una WLAN son:

- Implementación de una red de área local (LAN) en edificios de difícil acceso donde el cableado no es viable.
- Reconfiguración de una LAN en entornos cambiantes que necesitan una estructura flexible que se adapte a los cambios.

- Disponer de redes locales para situaciones de emergencia o congestión de la LAN alambrica
- Permitir el acceso a la información aunque el usuario este en movimiento.
- Implementación de una LAN a corto plazo para reuniones ad-hoc o de grupo de trabajo.
- Implementación en ambientes industriales de condiciones severas en los cuales se requiere interconectar dispositivos y maquinas.
- Interconexión de LANs que se encuentran en lugares diferentes.

Configuraciones de una WLAN

El grado de complejidad de las redes inalámbricas cuyo estándar base es el 802.11 varia dependiendo de las necesidades y requerimientos que se tengan, existen básicamente dos tipos de configuración:

- Modo ad-hoc.
- Modo infraestructura.

- Configuración peer to peer o ad-hoc

El modo ad-hoc, Fig. 2.5.7.1, es la configuración más sencilla, simplemente se tienen dos o más dispositivos cliente con su correspondiente tarjeta adaptadora para comunicaciones inalámbricas. Para que puedan comunicarse directamente sin el uso de un punto de acceso central entre ellos, es necesario que se vean de manera directa, esto es, que cada una de ellas este en el rango de cobertura radioeléctrica de la otra.

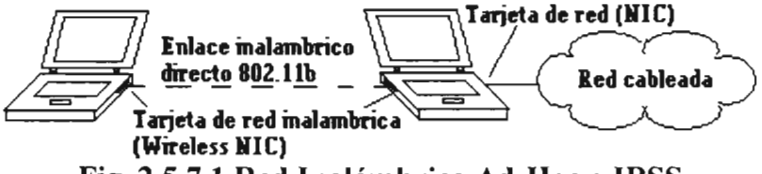


Fig. 2.5.7.1 Red Inalámbrica Ad-Hoc o IBSS

La configuración de la red inalámbrica de la Fig. 2.5.7.1 se conoce también como IBSS (Independent Basic Service Set) y si algún dispositivo necesita comunicación externa a la configuración IBSS una de las estaciones de trabajo debe operar como gateway, por lo que debe tener una segunda conexión de red y realizar ruteo. En este tipo de configuración no se requiere realizar tareas de administración.

- Configuración de infraestructura.

En el modo de infraestructura, Fig. 2.5.7.2 cada cliente se comunica a una estación central o punto de acceso AP (Access Point).

Esta configuración duplica el alcance de la red peer-to-peer ya que ahora la distancia máxima no es entre dos clientes sino entre cada cliente y el AP.

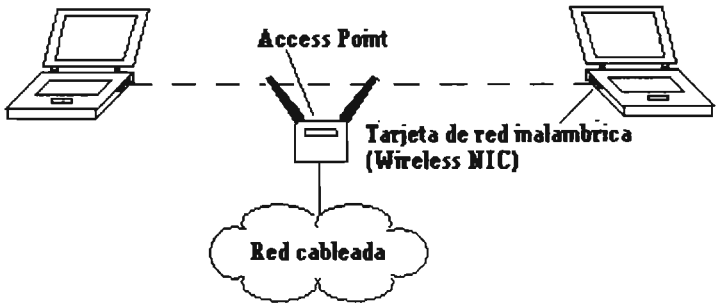


Fig. 2.5.7.2 Red inalámbrica BSS

La configuración de la Fig. 2.5.7.2 también se conoce como BSS (Basic Service Set) o red de área local inalámbrica (WLAN). El access point enlaza a los dispositivos inalámbricos a la red cableada, actuando como un hub, para esto tiene una conexión cableada a un switch en la red principal. Varios puntos de acceso se pueden configurar para proporcionar una gran área de cobertura mediante las celdas de cobertura que proporciona cada AP, estos AP se reparten la carga, proporcionan capacidad redundante y deben estar ligeramente solapados para permitir el paso de una celda a otra sin perder la comunicación.
Una tercera configuración es la que se usa para enlazar dos LAN que se encuentran por ejemplo en edificios diferentes como muestra la Fig. 2.5.7.3.

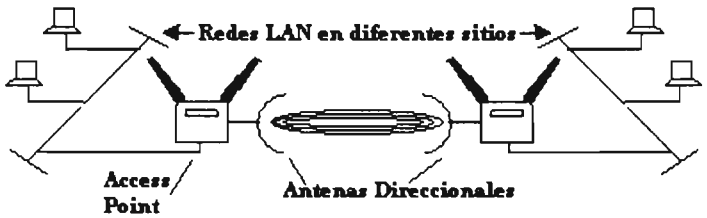


Fig. 2.5.7.3 Enlace entre varias LAN con tecnología inalámbrica

Esta configuración hace uso de antenas direccionales para enlazar redes que se encuentran en edificios diferentes. La antena direccional de cada edificio se apunta directamente a la otra para realizar el enlace, a su vez estas antenas se conectan a la red local mediante el AP.

Arquitectura del estándar IEEE 802.11

La arquitectura del estándar IEEE 802.11 referida al modelo OSI, Fig. 2.5.7.4, se compone de las capas física y de enlace.

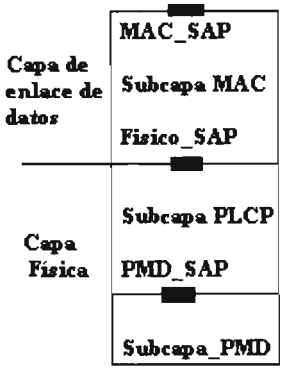


Fig. 2.5.7.4 Capas del estándar IEEE802.11

En la capa física tenemos dos protocolos:

- El protocolo PLCP (Procedimiento de Convergencia de Capa Física) que define la forma de mapear MPDUs o unidades de datos MAC en un formato de tramas para ser transmitidas o recibidas entre diferentes estaciones a través de la capa PMD. La función de este protocolo es implementar la convergencia de capa física que adapta las capacidades del sistema físico dependiente del medio (PMD).
- Un sistema PMD que define las características y la forma de transmitir y recibir a través de un medio sin cables entre dos o más estaciones.

La comunicación entre MACs de diferentes estaciones se realizara a través de la capa física mediante los SAPs, donde la capa MAC invocara las primitivas de servicio.

Tecnologías utilizadas para la transmisión en WLAN

Básicamente existen tres tecnologías de transmisión:

- Dos tecnologías de transmisión de espectro ensanchado.
- Tecnología de transmisión por infrarrojos.

- **Tecnología de transmisión de espectro ensanchado**

Esta tecnología difunde la señal de la información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una señal portadora reparte la señal por toda la banda disponible. Este ancho de banda se comparte con otros usuarios que trabajan en la misma banda frecuencial. Esta tecnología se subdivide en dos tipos:

- ❖ Tecnología de transmisión de espectro ensanchado por frecuencia directa DSSS (Direct Sequence Spread Spectrum).
- ❖ Tecnología de transmisión de espectro ensanchado por salto de frecuencia FHSS (Frequency Hopping Spread Spectrum).

- ❖ **Tecnología de transmisión de espectro ensanchado por frecuencia directa (DSSS).**

La tecnología de espectro ensanchado por frecuencia directa genera un patrón de bits redundante llamado señal de chip que se aplica a cada bit de la señal de información y después se modula la señal resultante mediante una onda portadora de radio frecuencia RF.

realizándose el proceso inverso en la recepción para recuperar la señal. Se usa una secuencia de bits para modular los bits de información conocida como secuencia de Barker, la cual tiene la forma:
+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1
Esta secuencia se aplica a cada bit de información, para el 1 binario y para el 0 binario en forma inversa como muestra la Fig. 2.5.7.5

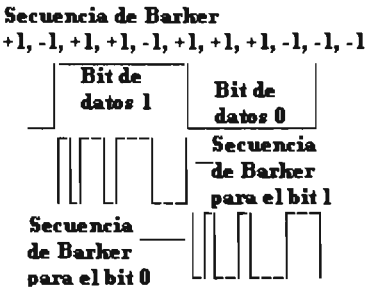


Fig. 2.5.7.5 Codificación de los bits de información mediante la secuencia de Barker

Una vez que se aplica la señal de chip, se modula la señal mediante alguna de las dos modulaciones existentes en DSSS. La modulación DBPSK (Differential Binary Phase Shift Keying) que proporciona una velocidad de transferencia de 1 Mbps y la modulación DQPSK (Differential Quadrature Phase Shift Keying) que proporciona una velocidad de transferencia de 2 Mbps.
La tecnología DSSS trabaja en la banda de frecuencias de 2,4-2,4835 GHz, es decir se tiene un ancho de banda de 83.5 MHz, este ancho de banda se divide en 14 canales de 5 MHz cada uno, de los cuales cada país usa un subconjunto de canales según sus normas. En topologías de red que contienen varias celdas solapadas o adyacentes pueden operar varios canales sin interferencia, siempre y cuando la separación entre frecuencias centrales sea como mínimo 30 MHz

- **Tecnología de transmisión de espectro ensanchado por salto de frecuencia (FHSS).**

La tecnología FHSS transmite una parte de la información con una determinada frecuencia durante un intervalo de tiempo inferior a 400 ms llamado dwell time. Cuando pasan los 400 ms se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. Así cada tramo de información se transmite a frecuencias diferentes en un intervalo de tiempo reducido, Fig. 2.5.7.6. Cada transmisión a una frecuencia concreta se realiza usando una portadora de banda estrecha que va cambiando a lo largo del tiempo. El orden en los saltos que el emisor realiza se determina en base a una secuencia pseudo aleatoria definida en una tabla que conocen tanto el receptor como el emisor. Este sistema tiene la ventaja respecto al DSSS de que puede tener más de un AP en la misma zona geográfica sin interferencia si se cumple que los dos puntos emisores usan una portadora diferente en un mismo instante.

Fig. 2.5.7.6 Salto de frecuencias de transmisión del sistema FHSS

En este sistema si se tiene una buena sincronización se transmitirá por diferentes canales físicos (las diferentes frecuencias de la portadora) pero por un solo canal lógico. Este sistema usa la modulación FSK con una velocidad de transmisión de 1 Mbps ampliable a 2 Mbps.

- **Tecnología de transmisión por infrarrojos.**

Los sistemas de infrarrojos utilizan altas frecuencias justo por debajo del tráfico de frecuencias de luz visible, no pueden pasar a través de objetos opacos pero sin embargo se pueden reflejar en ciertas superficies. La longitud de onda de operación se sitúa alrededor de los 850 a los 950 nm. Tienen una clasificación según el ángulo de apertura con el que se emite la información en el emisor:

- Sistemas de corta apertura o haz dirigido que funcionan como los controles remotos de los televisores, por lo que tanto el emisor y el receptor tienen que estar orientados antes de realizar la transmisión.
- Sistemas de gran apertura, reflejados o de difusión que radian la información en un rango un poco amplio, utilizan dos modulaciones: 16 ppm y la modulación 4 ppm quienes proporcionan 1 y 2 Mbps de velocidad respectivamente.

Hasta aquí hemos visto brevemente la parte física del estándar IEEE802.11, a continuación tenemos la capa de acceso al medio MAC.

Nivel de acceso al medio MAC

Los diferentes métodos de acceso al medio se diseñan según el modelo OSI y se sitúan entre la capa física y la parte inferior de la capa de enlace o subnivel MAC.

La capa MAC controla los aspectos como la sincronización y los algoritmos del sistema de distribución que forman el conjunto de servicios que propone el modo infraestructura.

La capa MAC se compone de dos funcionalidades:

- La función de coordinación puntual (PCF)
- La función de coordinación distribuida (DFC).

- La función de coordinación puntual (PCF)

La función de coordinación determina dentro de un conjunto básico de servicios (BSS) cuando una estación puede transmitir o recibir unidades de datos de protocolo (PDU) a nivel MAC a través del medio inalámbrico.

- La función de coordinación distribuida (DFC).

La función de coordinación distribuida (DFC) se encuentra en el nivel inferior del subnivel MAC la cual basa su funcionamiento en las técnicas de acceso aleatorias de contienda por

el medio. El tráfico que se transmite bajo DFC es del tipo asincrónico ya que las técnicas de contienda introducen retardos aleatorios y no predecibles que no pueden ser tolerados por los servicios sincronos. Las características de DFC son:

- Usa MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio.
- Usa reconocimientos (ACKs) por lo que existen retransmisiones si no se reciben los ACKs.
- Usa un campo Duration/ID que indica el tiempo de reserva para transmisión y ACK, de esta forma los nodos saben cuando el canal volverá a quedar libre.
- Concede prioridad a tramas mediante el espaciado de tramas IFS.
- Soporta broadcast y multicast sin ACKs.

Protocolo de acceso al medio (CSMA/CA) y MACA.

El algoritmo de acceso múltiple por detección de portadora con supresión de colisiones CSMA/CA (Carrier Sense Múltiple Access/Collisión Avoidance) funciona de la siguiente forma:

1. Antes de transmitir la estación prueba el medio o canal inalámbrico para determinar si esta libre u ocupado.
2. Si no esta ocupado realiza una espera adicional o espaciado entre tramas IFS.
3. Si durante este intervalo temporal o desde el principio el medio ya esta ocupado la estación espera hasta el final de la transacción actual para realizar alguna acción.
4. Cuando termina la espera, debido a que el medio estaba ocupado se ejecuta el algoritmo de backoff para determinar una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de backoff dará el numero aleatorio y entero de ranuras temporales para reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando para transmitir.
5. Mientras transcurre la espera marcada por el algoritmo de backoff se continua escuchando el medio para determinar si queda libre durante al menos un tiempo de IFS, la espera va avanzado hasta que la estación consume todas las ranuras asignadas. Si el medio no se libera durante un tiempo igual o mayor a IFS se suspende el algoritmo de backoff hasta que se cumpla la condición.

Este método de acceso (CSMA/CA) en los ambientes inalámbrico y celular presenta dos problemas básicos:

- Nodos ocultos. La estación detecta que el canal esta libre pero en realidad esta ocupado por otro nodo que no la escucha.
- Nodos expuestos. La estación cree que el canal esta ocupado cuando en realidad esta libre, ya que el otro nodo al que escucha no le interfiere para transmitir a otro destino.

Para tratar de solucionar los detalles anteriores el IEEE802.11 propuso el uso del protocolo de acceso múltiple con supresión de colisiones MACA (Múltiple Access Colision Avoidance), en el cual antes de transmitir el emisor envía una trama RTS (Request to Send) indicando la longitud de datos que desea enviar. El receptor contesta con una trama CTS (Clear to Send) repitiendo la longitud. Al recibir el CTS el emisor envía sus datos, en base a esto y para evitar los nodos expuestos y ocultos:

- Al escuchar un RTS hay que esperar un tiempo por el CTS.
- Al escuchar un CTS hay que esperar según la longitud.

El estándar IEEE 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

El tiempo que una estación escucha el medio (conocido como espacio entre tramas IFS) antes de transmitir se clasifica en 4 espaciados para dar prioridad de acceso al medio:

- SIFS (Short IFS). Es el tiempo más corto en el que se transmiten los reconocimientos y fragmentos de trama y es usado por el punto de control (PC) para enviar testigos a estaciones que quieran enviar datos síncronos.
- PIFS (PCF). Es utilizado por las estaciones para ganar prioridad de acceso en los periodos libres de contienda lo utiliza el PC para ganar la contienda normal que se produce al esperar DIFS.
- DIFS (DCF). Es el tiempo de espera habitual en el mecanismo MACA. En este tiempo se envían tramas MAC MPDUs y tramas de gestión MMPDUs.
- EIFS (Extended IFS). Realiza el control cuando llegan tramas erróneas, esperando un tiempo para que se vuelva a reenviar la trama.

Formato de las tramas MAC

Las tramas MAC se clasifican en tres tipos:

- Tramas de datos.
- Tramas de control. Son por ejemplo los reconocimientos ACKs, las tramas para multiacceso RTS y CTS y las tramas libres de contienda.
- Tramas de gestión. Estos tipos de trama son los servicios de distribución, las tramas de Beacon o portadora y las tramas TIM o de trafico pendiente en el punto de acceso

El formato genérico de la trama MAC se muestra en la Fig. 2.5.7.7

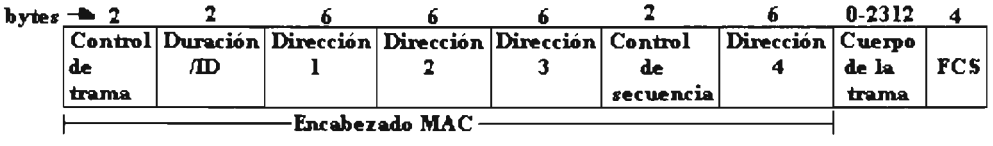


Fig. 2.5.7.7 Formato genérico de la trama MAC

Los campos de la trama son:

- Duration/ID. Se usa para señalizar el identificador de una estación con limitaciones de potencia. En el resto se utiliza para indicar la duración del periodo que ha reservado una estación
- Campos de dirección 1-4. Contienen las direcciones de 48 bits donde se incluyen las direcciones de la estación que transmite, la que recibe, el punto de acceso origen, y el punto de acceso destino.
- Control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se esta enviando.
- Cuerpo de la trama. Varía según el tipo de la trama que se quiere enviar.
- FCS. Contiene el checksum o verificación de que la trama llego correctamente.
- Campo de control. Los campos de control a su vez tienen otros subcampos como muestra la Fig. 2.5.7.8

	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
	Versión de Protocolo	Tipo	Subtipo	A DS	Desde DS	Mas Frag-mentos	Rein-tentar	Aminis-tración Potencia	Mas Datos	WEP	Orden
Bits	2	2	4	1	1	1	1	1	1	1	1

Fig. 2.5.7.8 Campos de control de trama

Los subcampos del campo control son:

- Tipo/Subtipo. El campo tipo indica si la trama es de datos, control o gestión. El campo subtipo identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- A DS/Desde DS. Identifica si la trama se envía o se recibe del sistema de distribución. En redes ad-hoc estos campos permanecen en cero. El caso más complejo es cuando se transmite entre dos estaciones a través del sistema de distribución. Para esto se sitúa a una de ellas tanto A DS como Desde DS.
- Más fragmentos. Se activa si usa la fragmentación.
- Reintentar. Se activa si la trama es una retransmisión.
- Power Management. Se activa si la estación entra al modo de economía de potencia.
- More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso
- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.
- Orden. Se usa con el servicio de ordenamiento estricto.

Características de las redes de área local inalámbricas:

- Las redes inalámbricas prestan esencialmente los mismos servicios que una red cableada tradicional.
- Son una opción ventajosa cuando la disposición física del lugar hace imposible la instalación del cableado.
- Las redes inalámbricas tienen gran flexibilidad debido a que no usan cableado, gracias a esto no se tienen problemas de reubicación de nodos por la movilidad que permite tener el sistema inalámbrico, la reubicación es inmediata, a diferencia del trabajo que implica mover un nodo en una red convencional.
- Son particularmente apropiadas para la utilización de computadoras portátiles o dispositivos de telemetría, con lo cual se puede tener gran movilidad sin sacrificar las ventajas de estar conectado a una red.
- Por lo general no requieren un gran ancho de banda.
- Roaming. Es un elemento en el diseño de redes inalámbricas a menudo muy olvidado. El roaming debe permitir a los usuarios con laptops o PDAs que se mueven a través del ambiente inalámbrico mantener la conectividad. Esto puede ser logrado a través del escaneo de clientes y el proceso de reasociación. La transición de un punto de acceso a otro debe realizarse entre transmisiones de paquetes para evitar la pérdida de datos en el paquete. Para asegurar el roaming debe haber suficiente traslapamiento en las celdas, al menos el 15% y que todos los AP se encuentren en la misma red, subred o VLAN.

Componentes de las redes de área local inalámbricas.

Los principales dispositivos para redes inalámbricas son:

- Interfaces de red

Estos dispositivos se instalan en los equipos PC´s, estaciones de trabajo, Laptops, etc., constan de una pequeña unidad de antena para la transmisión, los alcances varían con el ambiente y la frecuencia de operación pero van desde los 500 metros a 1 Mbps hasta los 160 metros a 11 Mbps en espacios abiertos.

La mayoría de estos dispositivos son para tecnología portátil (PCMCIA), algunos fabricantes venden adaptadores PCMCIA/ISA para la instalación en equipos de cómputo comunes. Estos dispositivos deben apegarse a las regulaciones de emisión electromagnética y deben ser seguros para ambientes domésticos.

- Nodos de acceso AP (Access Point).

Un access point AP es el punto central de una red de área local inalámbrica (WLAN). Es el equivalente de un hub sobre una red cableada, por lo que se encarga de proporcionar la conectividad. En él, es donde todas las señales se conectan para ser transportadas a una red más amplia, es decir el AP es el puente del trafico entre los dominios cableado e inalambrico por lo que necesitan situarse en puntos estratégicos donde se desea tener áreas de cobertura dentro de las cuales se efectuara la comunicación. Tienen tres modos de funcionamiento:

1. Modo root. En este modo el AP simplemente pasa el tráfico entre la red cableada y la inalámbrica, este es el modo por default.
2. Modo site survey. Es un modo de prueba para realizar estudios del sitio.
3. Modo repetidor. Cuando esta en modo repetidor la interfaz cableada del punto de acceso se encuentra en modo pasivo y el AP simplemente repite el trafico de un dispositivo inalámbrico a otro, sirviendo en este modo para agrandar la distancia que el rango de cualquier dispositivo cubre o sirve para rebotar una señal que rodee un obstáculo de la línea de vista de RF principal. Los AP en este modo deben tener un traslapamiento del 50% con el AP root. Como el AP es un dispositivo half duplex, debe mantener conexiones inalámbricas con el AP vecino por arriba y por debajo de el, con lo cual el rendimiento total se reduce a la mitad.

Algunas características de estos dispositivos son:

- Sus componentes son fijos o de antenas intercambiables.
- Su transmisión es del tipo half duplex.
- Puede autentificar usuarios y encriptar algunos datos.
- Generalmente usan una o dos interfaces de red que son idénticas a las que se colocan en los equipos PC por lo que pueden realizar segmentación de trafico sobre la misma área como si fueran bridges, esto permite hacer un uso eficiente del ancho de banda en ambientes concurridos.
- Tienen un puerto estándar ethernet 10BaseT o 10Base2 para conectarse a una red alambrica normal.
- Pueden colocarse arreglos de nodos de manera que se puedan implementar áreas de cobertura más grandes bajo un esquema similar al de telefonía celular donde se puede hacer roaming al pasar de un área a otra sin perder el acceso a la red.
- Se pueden configurar por consola, USB, interfaz Web o por un software de administración propietario.

- Nodos de ruteo y nodos de acceso remoto.

Estos dispositivos son nodos de acceso con funciones avanzadas, el nodo de ruteo puede hace ruteo de protocolos de nivel tres sobre canales inalámbricos distribuidos, los nodos de acceso remoto permiten tener sistemas de autenticación y contabilización con sistemas RADIUS.

- Antenas.

Las antenas o radiadores intencionales son los dispositivos que intencionalmente generan y emiten energía de radiofrecuencia por radiación o inducción para el propósito de comunicación.

Las antenas afectan tres propiedades fundamentales de las señales electromagnéticas: ganancia, dirección y polaridad.

La ganancia describe el incremento o decremento de la amplitud de la señal de radiofrecuencia.

La dirección describe la forma del patrón de transmisión. Las antenas pueden enfocar la energía de un access point para proporcionar un rango mas largo en cierta dirección con el costo de la perdida de cobertura en otras direcciones. Las antenas direccionales concentran e intensifican la radiofrecuencia (RF) en una dirección particular.

La polarización es la orientación física de la antena en una posición horizontal (el campo eléctrico es paralelo a la tierra) o vertical (el campo eléctrico es perpendicular a la tierra) de la antena. Las redes inalámbricas WLAN son configuradas típicamente con una polarización vertical. En este punto se debe hacer notar que las antenas deben ser polarizadas en la misma forma para que se comuniquen efectivamente. Las antenas pueden ser físicamente totalmente diferentes, con ganancias diferentes pero deben tener la misma polarización para que el enlace trabaje apropiadamente.

Las interfaces de red cuentan con su propia antena, así también los nodos de acceso usan las interfaces como transmisores por lo que no es necesario en condiciones normales usar algún dispositivo especial.

Pero cuando se requiere aumentar los rangos de cobertura hay diversas opciones en cuanto a antenas se refiere, hay antenas de tipo unidireccional, de diversos rangos de ganancia que permiten intercomunicar dos entidades, como dos edificios a través de un campus universitario y donde la distancia excede los rangos permitidos para las redes inalámbricas, existen también antenas de tipo omnidireccional, las cuales radian en todas direcciones a manera de radiodifusión con el fin de establecer enlaces de tipo punto multipunto entre varios edificios.

Básicamente existen tres tipos de antenas inalámbricas:

1. Antenas omnidireccionales (dipolo).
   Son el tipo más común de antena para un access point (AP), la cual radia energía igualmente en todas direcciones alrededor de un eje para proporcionar conectividad en todas direcciones sobre el plano horizontal. La energía radiante de la antena es concentrada en una región que parece como una dona sostenida en el pano horizontal con el dipolo atrancado verticalmente a través del hoyo en el centro de la dona.
2. Antena semidireccional.
   Esta antena direcciona la mayor parte de su energía en una dirección que en otras. A menudo radia en un patrón de cobertura hemisférico o cilíndrico. Ejemplos de

antenas semidireccionales son: match/panel (un tipo de antena plana diseñada para montaje en pared que radia un área de cobertura hemisférica) y Yagi (un tipo de antena direccional cilíndrica). Estos tipos de antenas son una buena opción para pasillos muy largos.

3. Antenas altamente direccionales.
   Antenas muy enfocadas a direcionar su energía en una dirección. Tienen un beamwidth muy estrecho y deben estar exactamente direccionadas una con otra. No proporcionan un área de cobertura para que los dispositivos del cliente las usen por lo que usualmente se instalan en enlaces punto a punto de gran longitud de entre 2 y 25 millas y usualmente vienen en uno de dos estilos, plato de rejilla y plato parabólico. En áreas de fuertes corrientes de aire se prefieren los platos de rejilla para que evadan la corriente de aire ya que los platos parabólicos pueden perder su alineación al atrapar las corrientes de aire y ser movidos por estas. Las distancias de cobertura de las antenas son afectadas por los siguientes factores:

- Máxima potencia de transmisión posible.
- Sensibilidad del receptor.
- Disponibilidad de una ruta no obstruida para la señal de radio.
- Ganancia máxima disponible para la antena.
- Perdidas del sistema (perdidas a través del cable coaxial sobre el que se desplaza la señal para la antena, conectores, etc.). Las perdidas son directamente proporcionales a la longitud del cable y generalmente inversamente proporcionales al diámetro del cable.
- Nivel de confiabilidad y disponibilidad deseadas del enlace.

Estas antenas altamente direccionales requieren especial atención a la zona Fresnel (área de forma elipsoide que ocupa una serie de áreas concéntricas rodeando la línea de vista (LOS), la cual depende de la longitud de la ruta de la señal y la frecuencia de la señal). Si la zona Fresnel de un enlace de radio frecuencia propuesto es bloqueada mas del 20%, o si una nueva construcción o los árboles bloquean la zona Fresnel de un enlace existente el elevar la altura de la antena puede aliviar el problema. La curvatura de la tierra puede ser un elemento que influye en enlaces excediendo las 7 millas. La tabla 2.5.7.1 muestra algunos tipos de antenas.

Tipo de antena	Horizontal Beamwidth	Vertical Beamwidth
Omnidirectional	360°	7-80°
match/Panel	30-180°	6.90°
Yagi	30-78°	14-64°
Parabolic Disk	4-25°	4-21°

Tabla 2.5.7.1 Tipos de antenas

En el caso omnidireccional se tienen rangos de cobertura entre 2.5 y 6 Km en un ambiente abierto y en el caso unidireccional pueden tener rangos desde 15 a 35 Km. La regulación limita a estos dispositivos a operar en campus no mayores a 3 Km.

- Amplificador.
  El amplificador es un dispositivo que incrementa la fuerza de la señal, compensado las perdidas que provocan ciertos dispositivos como cables particularmente largos. En estos dispositivos se debe observar que el parámetro EIRP cumpla las normas establecidas.

- Atenuador.
  Es un dispositivo que decrementa la fuerza de la señal a propósito, esto es por si el parámetro EIRP se sale de las normas permitidas.

- Splitter.
  Permite conectar dos antenas al mismo radio. Esto introducirá una cierta cantidad de perdidas que se reflejaran en las dos antenas.

- Software

Los nodos de acceso y en general las redes inalámbricas pueden administrarse y configurarse mediante software especializado donde entre otras cosas se realizan configuraciones particulares, diagnósticos del estado de los nodos, control de usuarios, servicios y monitoreo del estado del medio bajo interfaces graficas desde una o varias entidades en la red.
En algunos casos los fabricantes ofrecen soporte opcional a sistemas de seguridad alternativos como algoritmos DES.
También se tiene la opción de equivalencia de seguridad en redes inalámbricas WEP en los estándares IEEE 802.11. Los fabricantes ya soportan llaves de encriptación de 128 bits, la autenticación se da con certificados X509 y todos los tipos de autenticación prevalecientes en el mundo alambrico.

2.5.8 Protocolos de redes inalámbricas

Un grupo del IEEE tiene la misión de desarrollar los estándares para la operación de redes LAN inalámbricas dentro del esquema definido por las reglas y regulaciones del FCC (Federal Communications Committed). En 1977 el IEEE libero el estándar 802.11 para redes inalámbricas especificando trafico inalámbrico de 1 y 2 Mbps en la banda de los 2.4 GHz usando una de las dos técnicas de codificación: FHSS (Frequency Hopping Spread Spectrum) y DSSS (Direct Sequence Spread Spectrum). Se han realizado algunas extensiones al estándar original como muestra la tabla 2.5.8.1.

Estándar	Frecuencia	Velocidad Máxima	Canales disponibles	Interfaz De aire	Ancho de banda de canal
802.11	2.4 Ghz	2 Mbps		FHSS /DSSS	
802.11a	5 Ghz	54 Mbps	8 sin solapamineto	OFDM	25 MHz
802.11b (Wi-Fi)	2.4 Ghz	11 Mbps	11 solapados(Max. 3 concurrentes)	DSSS	25 MHz
802.11e	Proporciona calidad de servicio para 802.11a, 802.11b, 802.11g				
802.11g	2.4 Ghz	54 Mbps	11 solapados(Max. 3 concurrentes)	OFDM /DSSS	25 MHz
802.11i	Proporciona seguridad para 802.11a, 802.11b, 802.11g				
Hiperlan	5 Ghz	24 Mbps			
Hiperlan2	5 GHz	54 Mbps		OFDM	25 MHz
Bluetooth	2.4Ghz	1 Mbps			
HOME RF2	2.4 GHz	10 Mbps		FHSS	5 MHz
5-UP	5 GHz	108 Mbps		OFDM	50 MHz

Tabla 2.5.8.1 Principales estándares WLAN.

Donde:

- OFDM=Orthogonal Frequency División Multiplexing.
- 5-UP=5GHz Unified Protocol.

Estándar 802.11

El estándar o protocolo de redes inalámbricas 802.11 tiene las siguientes características.

- Especificación para velocidades de transmisión de 1 a 2 Mbps.
- Trabaja en la banda de frecuencia ISM de los 2.4 Ghz (2.4-2.848 GHz), sin necesidad de licencia.
- Usa la tecnología por salto de frecuencia (FHSS) o frecuencia directa (DSSS).
- Especifica la parte física y el acceso al medio.
- Soporta infrarrojos y radiofrecuencia.
- El método de acceso al medio es CSMA/CA.
- Soporta redes de computadoras portátiles y no portátiles.
- Sufre de interferencias con hornos de microondas, dispositivos bluetooth y teléfonos puesto que operan en el mismo espectro de frecuencias.

Estándar 802.11b

El estándar 802.11b también es conocido como Wi-Fi, fue el primero en ofrecer el ancho de banda necesario para hacer a las redes inalámbricas útiles. Sus características son:

- Maneja velocidades de datos de hasta 11 Mbps a distancias de 100 pies o más, esta distancia es desde un access point.
- Usa la tecnología DSSS.
- Opera en la banda de radio no licenciada de los 2.4 Ghz (2.4 a 2.483 Ghz).
- Un preámbulo es mandado inicialmente a la velocidad de 1 Mbps para asegurarse que hay una velocidad de datos común con cualquier receptor funcionando con un

protocolo más viejo. Una vez que el preámbulo ha sido mandado, la velocidad de datos cambiara a la velocidad especificada en el encabezado (usualmente 11 Mbps).
- Las ondas de radio de 2.4 Ghz tienen un mayor alcance que las frecuencias más altas, lo cual significa que el rango del estándar 802.11b llega mas lejos que el que esta disponible con 802.11 a.
- La banda de radio de 2.4 Ghz es muy utilizada con canales limitados disponibles y por lo que las WLANs compiten por el ancho de banda con teléfonos inalámbricos, Bluetooth, y otros dispositivos inalámbricos.
- Debido a que este estándar ha sido ampliametene instalado, se ha convertido en un lugar de ataque para los hackers.
- Es compatible con los equipos DSSS del estándar 802.11.

Estándar 802.11a

El estándar 802.11a maneja velocidades más altas cuyas características son:
- Trabaja a velocidad máxima de 54 Mbps
- Opera en el espectro de frecuencias de 5 Ghz sin necesidad de licencia, por lo cual no sufre por problemas de saturación por otras aplicaciones.
- Usa la codificación OFDM.

Estándar 802.11g

Las características del estándar 802.11g son:
- Maneja velocidades de transmisión 20 Mbps hasta un máximo de 54 Mbps.
- Opera en el espectro de frecuencias de 2.4 GHz sin necesidad de licencia.
- Usa las modulaciones DSSS y OFDM.
- Es compatible hacia atrás con los estándares 802.11b.
- Tiene mayor alcance y menor consumo de potencia que el 802.11a.

Estándar 802.11e

El objetivo de este estándar es proporcionar soporte de calidad de servico (QoS) para aplicaciones de redes WLAN. Tiene su aplicación en los estándares de redes inalámbricas IEEE802.11a, IEEE802.11b e IEEE802.11g. Proporciona clase de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

Estándar IEEE802.11i

Este estándar se estableció para cubrir el problema mas critico en las redes inalámbricas, la seguridad. Tiene aplicación en los estándares IEEE802.11a, IEEE802.11b e IEEE802.11g. También es una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación.

Estándar IEEE802.11d

Este estándar es un complemento al nivel de control de acceso al medio MAC para proporcionar el uso a nivel mundial de las redes WLAN, permitiendo a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

Estándar IEEE802.11f
El objetivo de este estándar es permitir la interoperabilidad de puntos de acceso (AP) dentro de WLAN multiproveedor. El estándar define el registro de un AP dentro de una red y el intercambio de información entre los AP cuando un usuario se traslada desde un AP a otro.

Estándar IEEE802.11h
Este estándar tiene el objetivo de cumplir con los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas.

Hiperlan
El Instituto de normalización europeo ETSI también ha realizado contribuciones para desarrollar especificaciones para redes inalámbricas con tasas de transferencia mayores que las del IEEE. El protocolo europeo se conoce como HiperLan ofrece cuatro estándares diferentes de los cuáles el tipo I se ajusta mucho a las necesidades futuras de las WLAN estimándose una velocidad de 23.5 Mbps. Otra especificación HiperLan/2 ofrece una mayor velocidad, 54 Mbps empleando el método de modulación OFDM (Orthogonal frequency División Multiplexing) además de contar con soporte de calidad de servicio. Sus características son:

- Especifica la parte física y el acceso al medio
- Velocidades de transmisión de 1 a 20 Mbps
- Usa las bandas de 5.15 a 5.25 GHz y de 17.1 a 17.3 GHz.
- Velocidad de transmisión de 54 Mbps usando la modulación OFDM para la transmisión de señales analógicas. Presenta gran efectividad en entornos con gran dispersión de señales.
- Soporta Infrarrojos y radiofrecuencia.
- El método de acceso al medio es CSMA/CA.
- El protocolo de acceso al medio MAC presenta un método duplex de división dinámica del tiempo para permitir una mayor eficiencia en la utilización de los recursos de radio.
- Los datos se transmiten en conexiones entre el terminal móvil MT y el punto de acceso AP con prioridades previamente establecidas Existen dos tipos de conexiones al igual que en IEEE 802.11, las conexiones punto a punto son bidireccionales y las punto a multipunto son unidireccionales con sentido hacia el MT.
- Permite asignar a cada conexión un nivel de prioridad respecto a otras conexiones, en ese nivel de prioridad se determinan parámetros como el ancho de banda a utilizar, el retraso máximo entre paquetes, tasa de errores, etc. Este soporte de calidad de servicio (QoS) combinado con la alta velocidad de transmisión permiten el flujo simultáneo de diferentes tipos de datos como video, voz y datos.
- Soporta redes de computadoras portátiles y no portátiles.

Estándar 802.15.1

Otra tecnología para redes inalámbricas es Bluetooth que describe un método de conectividad móvil universal con el cual se pueden interconectar dispositivos como teléfonos móviles, PDA, computadores y otros dispositivos utilizando una conexión inalámbrica de corto alcance.

Bluetooth soporta la transmisión de voz, video y datos y su funcionamiento consiste en que cada dispositivo se equipa con un pequeño chip que transmite y recibe información a 1 Mbps en la banda de frecuencias de 2.4 GHz y a una distancia operativa de 10 metros. Puede ofrecer acceso a Internet a través de las redes locales y soporte para la sincronización entre dispositivos informáticos.

El IEEE aprobó el estándar IEEE 802.15.1, el cual es compatible totalmente con la tecnología Bluetooth. En el estándar se definen las especificaciones de la capa física y MAC para redes WPAN (Redes de área personal inalámbricas). Anteriormente a la estandarización, los dispositivos Bluetooth no podían coexistir con los dispositivos basados en el IEEE 802.11b debido a que ambos se interferían entre si.

Las redes inalámbricas han resultado eficientes y baratas se ha incrementado la tasa de transmisión hasta 11 Mbps y se espera incrementar el ancho de banda al doble usando una técnica de modulación opcional especificada en el IEEE 802.11b, se pretende operar a una frecuencia de 7.5 GHz, ya se cuenta con una especificación a 5.7 GHz en el IEEE 802.11a, con una tasa de transmisión de 54 Mbps aunque se espera sea liberada hasta para 100 Mbps.

El éxito de las WLAN se basa en que usan frecuencias de uso libre por lo cual no es necesario pedir autorización o permiso para utilizarlas, aunque aun así se tiene que checar la normatividad de cada país. El problema con esas frecuencias es que son muy propensas a errores e interferencias. Una razón de errores del 50% provoca una reducción del caudal eficaz real o throughput de dos terceras partes. De esta forma si se dice que la velocidad de transmisión máxima de IEEE 802.11b es de 11 Mbps el máximo throughput será de 6 Mbps o menos.

Las soluciones de WLAN ya están disponibles actualmente con una atendencia creciente, con prometedores anchos de banda para permitir variadas aplicaciones, aunque aun tienen que vencer los obstáculos que imponen la seguridad y la interferencia.

3. PROTOCOLOS DE INTERNET

3.1 TCP/IP

El Protocolo de Control de Transmisiones/Protocolo Internet (TCP/IP) es un conjunto o familia de protocolos de comunicaciones abiertos y normalizados desarrollados para intercomunicar computadoras de cualquier red o fabricante y permitir su cooperación y compartición de recursos a través de la red respetando los protocolos de cada red individual. El conjunto se diseño teniendo en cuenta la existencia de muchas redes que tiene como elemento básico de interconexión los gateways o routers. De este conjunto de protocolos los más conocidos son TCP e IP de ahí el nombre generalizado del conjunto como TCP/IP.
El modelo de referencia TCP/IP y su pila de protocolos hacen posible la comunicación entre computadores en cualquier parte del mundo. Es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporciona una abstracción total del medio.
TCP/IP se popularizo gracias a muchos factores, entre ellos los dos principales fueron:

- Fue desarrollado por la DARPA (Agencia de proyectos de investigación avanzada de los EE.UU.).
- Internet. TCP/IP nace como un proyecto de investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El objetivo de esta investigación era la interconexión de redes (Internetworking), con esto se originó la creación de una gran red de redes de computadoras, la red Internet.

Para comunicar las redes se desarrollaron varios protocolos:

- El protocolo de Internet (IP) y los protocolos de control de transmisión (TCP) los cuales se englobaron en el conjunto de protocolos TCP/IP. Este conjunto de protocolos funciona ahora como un estándar en la red de redes Internet.

Organismos de estandarización de TCP/IP.
Para el estudio de estos protocolos se han creado algunas sociedades conocidas como las Sociedades de TCP/IP e Internet:

- La sociedad de Internet ISOC (Internet Society) es una organización mundial que se encarga de la interconexión entre las redes y aplicaciones de Internet.
- La IAB (Internet Architecture Board) es una organización dependiente de la ISOC y su función principal es estandarizar los protocolos de Internet, publicar los RFCs y gobernar a las siguientes sociedades:
    - IETF (Internet Engineering Task Force). Desarrolla los estándares y protocolos de Internet, vigila y desarrolla soluciones a problemas técnicos acerca de Internet. Esta organización hace concertaciones con desarrolladores de soluciones para Internet y resuelve problemas técnicos.
    - IANA (Internet Assigned Number Authority). Revisa y coordina las asignaciones únicas de los protocolos de Internet (direcciones IP).
    - IRTF (Internet Research Task Force). Se encarga de los nuevos proyectos con TCP/IP (como IPV6).

Los RFCs (Request for comments) son las publicaciones de los estándares de TCP/IP, estos publican los protocolos enumerados, documentados y clasificados según su utilidad, se clasifican en los siguientes 5 tipos:

- Requerido. Son los RFCs que son mandatarios y que por lo tanto se debe apegar a ellos. Deben ser implementados en todas las maquinas que ejecuten TCP/IP incluso gateway y routers.
- Recomendado. Se estimula a que todas las maquinas que ejecuten TCP/IP utilicen esta especificación de RFC. Normalmente son usadas en todas las maquinas
- Electivo. Son RFCs opcionales.
- De uso limitado. No son de uso tan extendido o general.
- No recomendado. No se aconseja su uso.

Modelo TCP/IP vs. modelo de referencia OSI.

Los protocolos TCP/IP se crearon y normalizaron mucho antes de que se definiera el modelo de referencia OSI de ISO, por lo que la arquitectura de redes basada en TCP/IP difiere un poco del modelo OSI, Fig. 3.1.1.

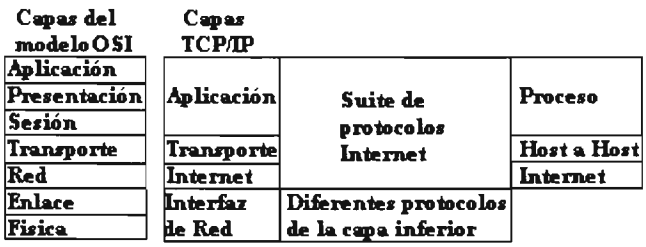


Fig. 3.1.1. Capas del Modelo de referencia de OSI vs. Capas TCP/IP

El modelo TCP/IP se basa en el funcionamiento de las redes de conmutación de paquetes. Propone cuatro capas en las que las funciones de las capas de sesión y presentación son responsabilidad de la capa de aplicación. El conjunto de protocolos que forman a TCP/IP especifica las funciones correspondientes a las capas del modelo OSI por encima de la capa de enlace de datos.

Niveles de TCP/IP

En la Fig. 3.1.1 se puede ver que el modelo TCP/IP se compone de 4 niveles:

- Nivel de interfaz de red.
- Nivel de Internet.
- Nivel de transporte.
- Nivel de aplicación.

Nivel de interfaz de red

TCP/IP no considera no considera al nivel físico como un componente de su arquitectura y tiende a agrupar la capa física con la capa de enlace, así las capas de enlace de datos y física son vistas como la capa de interfaz de red, esta es la base del modelo TCP/IP. La capa de interfaz de red o de acceso a la red comprende el nivel de enlace y buena parte del nivel de red. Este nivel es el responsable del intercambio de tramas (frames, paquetes de información que viajan en una red como una unidad simple) entre dos sistemas conectados a una misma red, controla la interfaz entre un sistema final y una subred, cubre los aspectos

que requiere un paquete IP para realizar un enlace físico, incluye detalles de tecnología de LAN y WAN.
El nivel de enlace es el responsable de proveer los siguientes servicios a la capa de enrutamiento:

- Delimita el principio y fin de las tramas a ser enviadas.
- Establece el sistema de direccionamiento físico de la red. Uno de los principales elementos que maneja esta capa es el de direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red y que son el medio principal de localización de un host dentro de una red. Cada tarjeta tiene un identificador, de la cual los 3 primeros bytes son asignados por el fabricante, los otros 3 se asignan de manera especial. Cuando un host debe enviar un paquete a otro host dentro de su red lo busca mediante su número de tarjeta de red (dirección física).

La capa de enlace puede ofrecer un servicio de conexión orientado o un servicio de conexión no orientado.
Si en la arquitectura de TCP/IP se distinguiera una capa física esta coincidiría exactamente con la capa física del modelo OSI. La capa física tiene la función de hacer uso de la línea de transmisión para el envío y la recepción de los bits contenidos en una trama, no especifica ningún tipo de protocolo o función en la capa de enlace de datos. TCPIP aprovecha que existen ya muchos estándares a nivel de enlace que permiten el acceso al medio, los estándares más usuales que componen esta interfaz de red son los del proyecto IEEE 802. El motivo de no definir protocolos de la capa inferior es para permitir a los protocolos de Internet interoperar con diversas tecnologías físicas y de enlace.
La unidad de envío o recepción de datos de la capa de enlace es la trama y los de la capa física son los bits que componen a la trama.
De la suite de protocolos TCP/IP los que operan en los niveles más bajos son ARP y RARP.

Nivel de Internet

La capa de red o nivel de Internet se superpone a la red física creando un servicio de red virtual independiente de aquella. No es confiable ni orientado a conexión. Este nivel comprende el resto del nivel 3 de OSI no incluido en la capa de interfaz de red. El propósito de la capa de Internet es enviar paquetes origen encapsulados en datagramas desde cualquier red y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí, para ello ejecuta todos los algoritmos de enrutamiento para determinar la mejor ruta a seguir y la conmutación de paquetes. Las funciones principales de la capa de red o servicios que proporciona a la capa de transporte son:

- Conectar equipos que están en redes diferentes.
- Permitir que los datos atraviesen distintas redes interconectadas.
- Establecer el sistema de direccionamiento lógico de la red y de los datagramas, así como facilitar la identificación de los nodos en la red en sentido lógico.
- Enrutamiento y segmentación de paquetes. Si un paquete que va a ser enrutado excede la máxima unidad de transferencia MTU (Maximum Transfer Unit) de un enlace este nivel fragmenta el paquete con el fin de adaptarlo al MTU del enlace y el paquete es ensamblado en el destino.

La unidad de datos que envía o recibe este nivel es el datagrama IP. El nivel de Internet realiza su mejor esfuerzo para entregar los datagramas, los paquetes introducidos en la red

por los hosts viajan independientemente al destino con los datos necesarios para el envío, por lo que no hay garantías de entrega ni de orden, por lo tanto pueden perderse, duplicarse o cambiar de orden. Dos son los protocolos más comunes de esta capa que son ICMP e IP. El protocolo IP proporciona el ruteo y control de congestión, el proceso de enrutamiento hace uso de un servicio no orientado a conexión para el envío y recepción de paquetes.

Nivel de transporte

El nivel de transporte proporciona a las aplicaciones servicios de comunicaciones y permite el establecimiento de sesiones o la comunicación entre pares de aplicaciones desde la estación emisora hasta la receptora, es decir conexiones de host a host o extremo a extremo mediante la definición de puntos terminales denominados puertos, en estos puertos las aplicaciones están escuchando a la red en espera de peticiones de conexión. Este nivel se asegura que los datos llegan en el mismo orden en que han sido enviados y sin errores para ello maneja aspectos como la confiabilidad, el control de flujo y la corrección de errores. También realiza un control extremo a extremo mediante el uso de ventanas deslizantes y la confiabilidad proporcionada por el uso de números de secuencia y acuses de recibo, corrige aspectos que no cubre el nivel de Internet IP al miso tiempo que utiliza los servicios de esta capa para proporcionar un servicio eficiente y confiable a los procesos de la capa de aplicación, es por ello que no se preocupa de la ruta que van a seguir los datos para llegar a su destino final, considera que la comunicación entre ambos extremos esta ya establecida y la utiliza, este nivel incluye mecanismos de seguridad..

Este nivel ofrece dos servicios a la capa de aplicación:

- Un servicio consiste en el envío y recepción de datos orientado a conexión, es decir, primero se intercambian tramas entre las maquinas implicadas para iniciar la comunicación y luego se intercambian los datos.
- El otro servicio consiste en el envío y recepción de datos no orientados a conexión, aquí la transmisión es directa, se empiezan a enviar tramas a la maquina destino sin antes haber iniciado ningún tipo de acuerdo.

Dos son los principales protocolos de esta capa:

- TCP. El protocolo de control de transmisión TCP es un servicio orientado a conexión y confiable. La unidad de datos que envía o recibe el protocolo TCP se llama segmento TCP.
- UDP. El protocolo de datagramas de usuario UDP es un servicio no orientado a conexión y no confiable. La unidad de datos que envía o recibe el protocolo UDP es el datagrama UDP.

Se puede utilizar uno u otro protocolo dependiendo del método preferido de envío de datos.
En esta capa se produce la segmentación de los datos producidos en la capa de aplicación en unidades de menor tamaño llamadas paquetes o datagramas. Un datagrama es un conjunto de datos que se envía como un mensaje independiente.

Nivel de aplicación

El nivel de aplicación proporciona comunicación entre procesos de usuario o aplicaciones entre computadoras distintas, además de las aplicaciones se ocupa de los detalles de las capas de sesión y presentación. En la capa de aplicación se manejan protocolos de alto nivel, protocolos de gestión, de transferencia, de búsqueda y de acceso, maneja aspectos de representación, codificación y control de dialogo. En esta capa hay un gran número de

protocolos, los cuales son considerados como protocolos de proceso que proveen servicios de aplicación, presentación y sesión.
Por ejemplo tenemos como protocolos de proceso que hacen uso del protocolo TCP del nivel 4: Telnet, FTP, http, SMTP, RIP, etc. los cuales proporcionan servicios de aplicación como NFS, XDR y RPC.
Entre los más usados con el protocolo UDP del nivel 4 están SNMP, TFTP.
Las aplicaciones utilizan un modelo cliente servidor en las comunicaciones.
Un servidor es una aplicación que ofrece un servicio a usuarios de Internet, un cliente es el que pide ese servicio. Una aplicación consta de una parte servidor y parte cliente que se pueden ejecutar en el mismo sistema o en diferentes sistemas. Los usuarios son la parte cliente de la aplicación, que construye una solicitud para ese servicio y se la envía al servidor de la aplicación que usa TCP/IP. El programa servidor recibe la solicitud, realiza el servicio requerido y devuelve los resultados en forma de respuesta.
El servidor puede manejar múltiples peticiones al mismo tiempo. Los servidores esperan las solicitudes en puertos bien conocidos de modo que sus clientes saben a que socket IP deben dirigir sus peticiones. El cliente por su parte emplea un puerto arbitrario para comunicarse. Los clientes que se quieren comunicar con un servidor que no usa un puerto bien conocido tienen un mecanismo para saber a que puerto dirigirse como Portmap que usa un servicio de registro el cual usa puertos bien conocidos.
La Fig. 3.1.2 muestra los diferentes niveles de TCP/IP con sus mensajes intercambiados entre niveles.

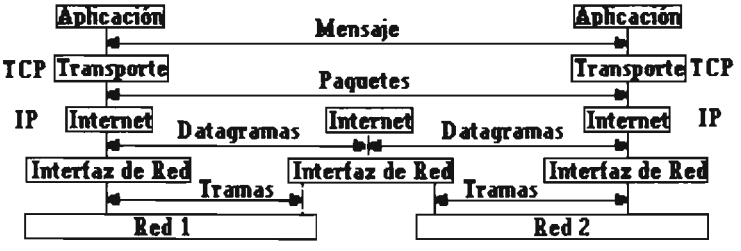


Fig. 3.1.2 Mensajes de los niveles TCP/IP.

De la Fig. 3.1.2 se observa que las aplicaciones se comunican mediante mensajes, el nivel de presentación se implementa en la aplicación. El nivel de transporte implementa algunas funciones del nivel de sesión mediante paquetes. El nivel Internet maneja los niveles de red mediante la interfaz de red que usa el intercambio de datagramas.
La arquitectura que los protocolos de TCP/IP proponen para comunicar redes es la clave para entender su funcionamiento. La arquitectura ve como iguales a todas las redes que se conectan, sin tomar en cuenta su tamaño o que sean locales o de cobertura amplia. Todas las redes que intercambian información deben estar conectadas a un mismo equipo de procesamiento conocido como compuerta o ruteador. Las computadoras deben estar identificadas con precisión, ya sea a nivel bajo (dirección física) o a nivel alto (dirección lógica) dependiendo del protocolo que se utiliza. TCP/IP usa un identificador conocido como dirección de Internet o dirección IP, que tiene una longitud de 32 bits y que identifica tanto a la red a la que pertenece la computadora como a la computadora misma.
Las características de TCP/IP son:

- Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones.

- La red es del tipo de conmutación de paquetes y se basa en un nivel de Internet sin conexiones. La conmutación de paquetes se realiza entre nodos.
- El conjunto de protocolos que lo integran son estándares.
- Existe un conjunto común de programas de aplicación.
- Realiza reconocimientos de extremo a extremo.
- En el nivel de red los protocolos son no orientados a conexión.
- Las redes se comunican mediante routers y son vistas como iguales.
- Es independiente de la tecnología usada a bajo nivel, del fabricante y de la arquitectura de la computadora.
- Es ruteable.
- Funciona en maquinas de cualquier tamaño.
- Permite el acceso a Internet.
- Permite la conectividad universal a través de la red.
- Trabaja en el ambiente cliente/servidor, que es el ambiente básico en Internet.
- La arquitectura de Internet esta basada en capas.
- TCP/IP es multiplataformas ya que trabaja en ambientes heterogéneos gracias a sus características de seguridad, confiabilidad, rentabilidad, ruteabilidad, y su acceso a Internet.

Los protocolos TCP/IP proporcionan servicios de comunicación universales como:

- Transferencia de archivos.
- Login remoto o terminal virtual.
- Correo electrónico.
- Acceso a archivos distribuidos.
- Administración de sistemas.
- Manejo de ventanas.

Arquitectura TCP/IP

A diferencia del modelo OSI en TCP/IP no existe un modelo oficial de protocolos, ya que estos se han ido definiendo anárquicamente y posteriormente se han englobado en capas. La arquitectura TCP/IP propone cuatro capas en las que las funciones de las capas de sesión y presentación son responsabilidad de la capa de aplicación y las capas de liga de datos y física con vistas como la capa de interfaz a la red. TCP/IP presupone independencia del medio físico de comunicación ya que existen estándares al nivel de enlace de datos y físico que proporcionan mecanismos de acceso a los diferentes medios y que TCP/IP los considera la capa de interfaz de red, los más usuales son el proyecto IEEE802: Ethernet, Token Ring y FDDI.

El funcionamiento de TCP/IP se centra en un equipo que maneja IP, en este caso es el router o gateway que se encarga de encaminar la información entre redes diferentes, Fig. 3.1.3.

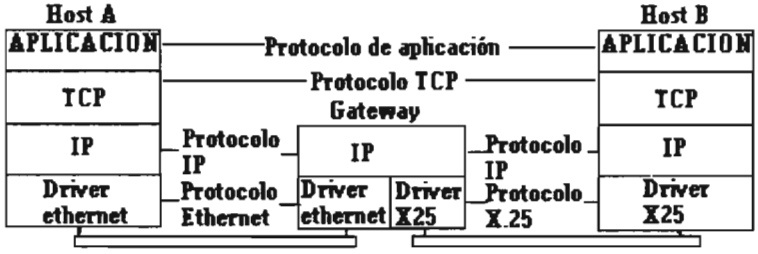


Fig. 3.1.3 Interconexión de redes diferentes mediante un gateway

Para que las estaciones se comuniquen deben tener implementado el protocolo IP, cada red a la que pertenezca la estación se conoce como una subred. Cada equipo implementa un nivel físico, otro de acceso al medio, uno de IP, otro de TCP y pueden desarrollar varios niveles de aplicaciones. Para que las aplicaciones en las dos estaciones se comuniquen requieren tener dos direcciones cada una, una es la dirección IP de la maquina y la otra es la dirección del puerto que se refiere a cada aplicación de la estación. La información de los protocolos superiores se encapsula en la información de los protocolos inferiores. Cada capa del modelo TCP/IP agrega una cabecera a los datos del nivel de aplicación, Fig. 3.1.4

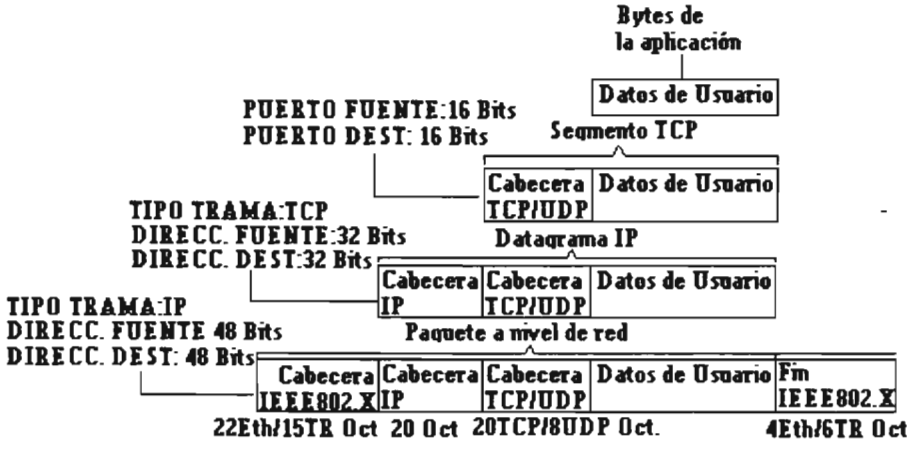


Fig. 3.1.4 Encapsulamiento de los datos en TCP/IP

La cabecera TCP incluye en su cabecera los campos:

- Puerto destino: Puerto al que va dirigida la comunicación.
- Número de secuencia: para reordenar la información en el destino
- Suma de comprobación: para detectar errores en la transmisión.

IP añade en su cabecera la información referente al encaminamiento.

La capa de acceso a la red normalmente Ethernet introduce entre otros campos la capa de acceso a la subred.

3.1.1 Protocolos TCPIP

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde la comunicación de más bajo nivel como es la transmisión de un flujo de bits a un medio hasta las comunicaciones de más alto nivel como es la compartición o transferencia de información de una computadora a otra en la red.
Mas de 100 protocolos integran actualmente a TCP/IP, en sus inicios eran 25, implementan funciones a todos los niveles de las capas OSI excepto el físico, como muestra el grafico de protocolos de la Fig. 3.1.1.1.

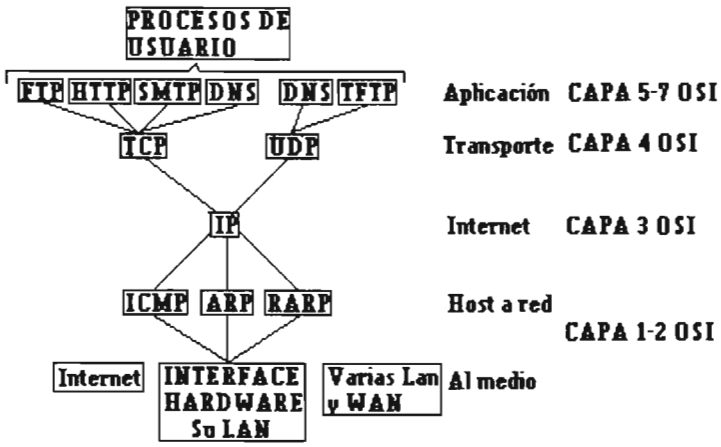


Fig.3.1.1.1 Grafico de protocolos más comunes en TCP/IP

El diagrama de la Fig. 3.1.1.1 conocido como grafico de protocolos ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP
Normalmente a este conjunto de protocolos suele hacerse referencia como si fueran uno solo, comúnmente escuchamos decir el protocolo TCP/IP, esto se debe a que el conjunto de protocolos TCP/IP surgieron de dos conjuntos previamente desarrollados que son: los protocolos de control de transmisión TCP (Transmition Control Protocol) e Internet IP (Internet Protocol), estos dos protocolos que lo componen son los de más amplio uso. Mencionamos que suele hacerse referencia a estos protocolos como uno solo (TCP/IP) pero como este conjunto contiene a uno de los protocolos mas usados también suele hacerse referencia a ese conjunto como el protocolo IP.
Los protocolos que componen la pila TCP/IP se pueden clasificar como:
- Protocolos ruteables.
- Protocolos de ruteo.
- Protocolos de control.
- Protocolos de aplicación.

La suite de protocolos de TCP/IP se muestra en la Fig. 3.1.1.2

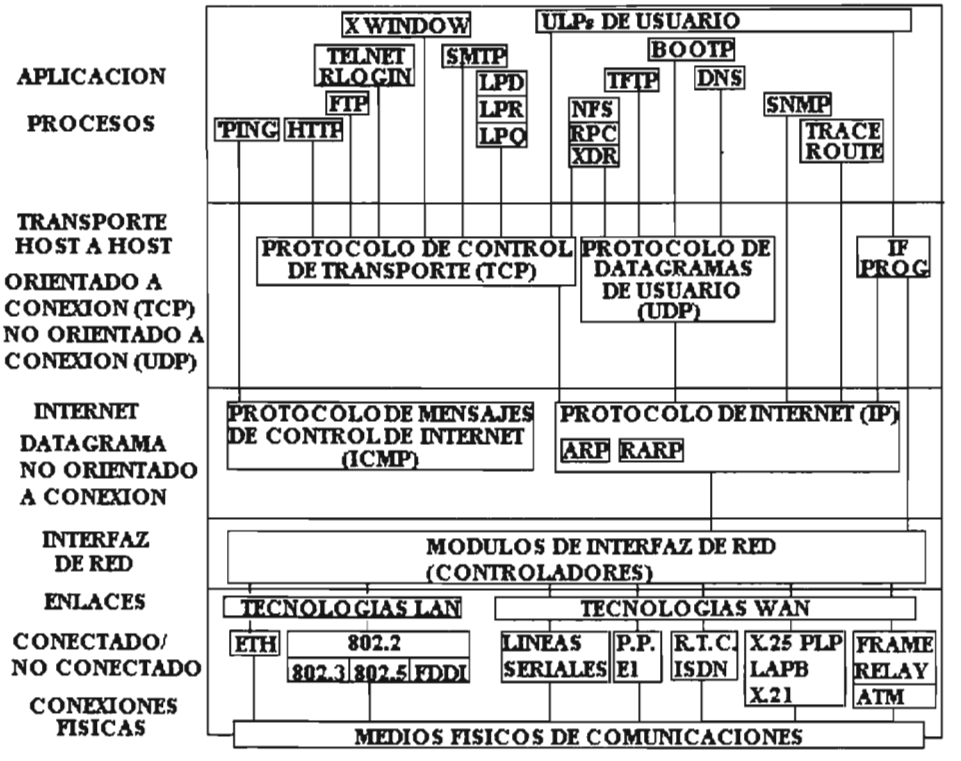


Fig. 3.1.1.2 Pila de protocolos TCP/IP

Algunos de los protocolos que componen la suite se listan en la tabla 3.1.1

Protocolos de capa 1 y 2	
Protocolo ARP	Protocolo RARP
Protocolos de tunelización	
ATMP Ascend Tunel Management Protocol	L2F Layer 2 forwarding Protocol
L2TP Layer 2 tunneling Protocol	PPTP Point to point tunneling Protocol
Protocolos Capa de Internet	
IP/IPv6 Internet Protocol	DHCP/DHCPv6 Dynamic Host Configuration Protocol
ICMP/ICMPv6 Internet Control Message Protocol	IGMP Internet Group Management Protocol
PIM: Protocol Independet Multicast	
RSVP: Resource ReserVation setup Protocol	
Seguridad	
AH: Authentication Header	ESP: Encapsulation Security Payload
Ruteo	
BGP-4: Border Gateway Protocol	EGP: Exterior Gateway Protocol
EIGRP: Enhance Interior Gateway Protocol	GRE: Generic Routing Encapsulation
HSRP: Cisco Hot Standby Router Protocol	IGRP: Interior Gateway Routing Protocol
NARP: NBMA Address Resolution Protocol	NHRP: Next Hop Resolution Protocol
OSPF: Open Shortest Path First	RIP/RIPv6: Routing Information Protocol
Transporte	
TCP: Transport Control Protocol	UDP: User Datagram Protocol
Mobile IP	Compressed TCP
XOT: X25 sobre TCP	
Voz sobre IP	
MGCP: Media Gateway Control Protocol	SGCP: Simple Gateway Control Protocol
Aplicación	
DNS: Domain Name Service	NetBIOS/IP
FTP: File Transfer Protocol	TFTP: Trivial File Transfer Protocol
FINGER: User Information Protocol	Gopher: Internet Gopher Protocol
HTTP: Hypertext Transfer Protocol	S-HTTP:Secure Hypertext Transfer Protocol
IMAP4: Internet Message Access Protocol rev 4	IPDC: IP Device Control
ISAPMP: Internet Key EXCHANGE	NTP: NetworkTime Protocol
POP3: Post Office Protocol version 3	Radius
RLOGIN: Remote Login	RTSP: Real Time Stream Protocol
SMTP: Simple Mail Transfer Protocol	SNMP: Simple Network Management Protocol
TACACS+; Terminal Access Controller Access Control System	Telnet
X-Window	

Tabla 3.1.1.1 Suite de protocolos TCPIP

A continuación describiremos brevemente algunas funciones de los protocolos más usados o conocidos de la suite de protocolos TCP/IP.

Protocolos de capa física

TCP/IP no específica claramente un protocolo de nivel de enlace de datos por lo que son necesarios algunos mecanismos para traducir direcciones IP a direcciones que entienda el software de la capa de enlace de datos sobre el que corre TCP/IP y para controlar posibles errores a nivel de subred. Realmente TCP/IP hace uso de los protocolos existentes a nivel de enlace, en el caso de redes de área local toma los protocolos estandarizados por el proyecto 802.x del IEEE.

Algunos protocolos que se pueden manejar en la capa de enlace son:

- **Protocolo ARP.**

Es un protocolo que se encarga de convertir las direcciones IP en direcciones de red física[1].

- **Protocolo RARP.**

Protocolo usado en la inicialización de las computadoras para que una vez que envían su dirección física obtengan de un servidor RARP su dirección IP correspondiente[1].

- **Protocolo L2F**

El protocolo L2F permite la tunelización de la capa de enlace de los protocolos de capas superiores. Con él, es posible separar la localización inicial del servidor de marcación de la localidad en la cual el protocolo de conexión de marcación es terminado y accesa a la red proporcionada, el formato del paquete es el de la Fig. 3.1.1.3.

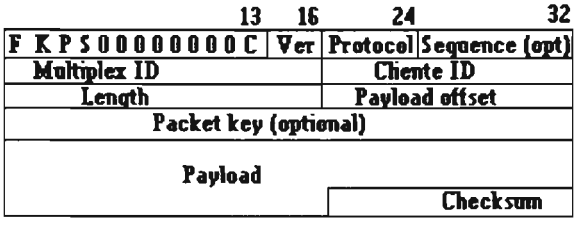


Fig. 3.1.1.3 Formato del paquete L2F

Sus campos son:

- Versión: La versión más reciente del software L2F que crea el paquete.
- Protocol: Especifica el protocolo transportado dentro del paquete L2F.
- Secuencia: El numero de secuencia esta presente si el bit S en el encabezado L2F es puesto a 1.
- Multiplex ID: El paquete multiplex ID identifica una conexión particular dentro de un túnel.
- Cliente ID: El cliente ID asiste a los extremos en la demultiplexación de túneles.
- Longitud: La longitud es el tamaño en octetos del paquete entero, incluyendo el encabezado, todos los campos y la carga útil (payload).
- Payload offset: Especifica él numero de bytes mas alla del encabezado L2F al cual el dato de la carga útil se espera empiece. Es habilitado si el bit F es puesto a 1.

[1] Estos protocolos se verán con mas detalle en el tema 3.2

- Paquete clave: El campo clave esta presente si el bit K es establecido en el encabezado L2F. Esto es parte del proceso de autentificación.
- Checksum: Es la suma de comprobación del paquete, es habilitado por el bit C=1.

- **Protocolo L2PT**

Este protocolo es usado para integrar servicios de marcación multiprotocolo en ISPs, puede ser usado para resolver el problema de división del grupo de captura multienlace. Multilink PPP a menudo es usado para agregar canales ISDN-B, requiere que todos los canales que componen un lote de multienlace sean agrupados en un servidor de acceso de red (NAS). Por que L2PT hace que una sesión PPP aparezca en una localidad mas que el punto físico en el cual la sesión fue físicamente recibida, puede ser usado para hacer que todos los canales aparezcan como un solo NAS, permitiendo una operación multienlace aun cuando las llamadas físicas son distribuidas a través de distintos NAS físicos. El formato del paquete es el mostrado en al Fig. 3.1.1.4.

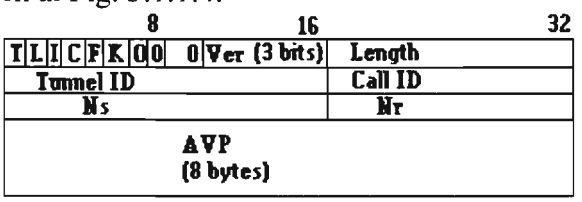


Fig. 3.1.1.4 Estructura del paquete L2PT

Campos:

- T: El bit es 1 para mensajes de control y 0 para mensajes de carga útil. Para mensajes de control los siguientes 7 bits se ponen a 1001000, haciendo el encabezado más compatible en la codificación con el mensaje de carga útil.
- L: Cuando es establecido indica que el campo longitud esta presente, indicando la longitud total del paquete recibido. Debe ser establecido para mensajes de control.
- I y C: Reservados y puestos a 0.
- F: Si es establecido, los campos Ns y Nr estan presentes. Debe ser establecido para mensajes de control.
- K: reservado y puesto a 0.
- O: indica que 1 campo tamaño de compensación esta presente en los mensajes de carga útil.
- Ver: Debe ser 002, indica la versión 1 del mensaje L2PT.
- Length: Longitud total del mensaje incluyendo encabezado, tipo de mensaje AVP, más cualquier AVP adicional asociado con un tipo de mensaje de control dado.
- Túnel ID: Identifica el túnel al cual un mensaje de control aplica. Si un túnel ID asignado no ha sido recibido de la otra punta, este campo debe ser puesto a 0. Una vez que un túnel ID asignado es recibido, todos los paquetes adicionales deben ser mandados con el túnel ID puesto al valor indicado.
- Call ID: Identifica la sesión de usuario dentro de un túnel al cual un mensaje de control aplica. Si un mensaje de control no aplica a una simple sesión de usuario dentro del túnel debe ser puesto a 0.
- Nr: Paquete transmitido actualmente.
- Ns: Ultimo Paquete transmitido.
- AVP: EL AVP (Attribute-Value Pair) es un método uniforme usado para codificar tipos de mensaje y cuerpos de principio a fin L2PT.

- **Protocolo PPTP**

El protocolo de tunelización punto a punto permite al protocolo PPP ser encauzado a través de una red IP. Usa una arquitectura cliente-servidor para desacoplar funciones que existen en servidores de acceso a red y soporta VPNs. Especifica un protocolo de control de llamada y administración que permite al servidor controlar el acceso para marcación de llamadas de circuitos conmutados originándose de una PSTN o una ISDN o para iniciar conexiones de circuitos conmutados de salida. Usa un mecanismo de encapsulamiento de ruteo genérica para proporcionar servicios de datagramas encapsulados de flujo y congestión controlados para transportar paquetes PPP. El formato del encabezado es mostrado en la Fig. 3.1.1.5.

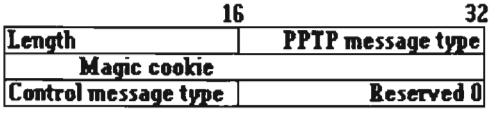


Fig. 3.1.1.5 estructura del encabezado PPTP

- Length: Longitud total en octetos del mensaje PPTP incluye el encabezado.
- Message type: Los dos posibles valores del tipo de mensaje son: Mensaje de control y mensaje de administración.
- Magic cookie: Tiene un valor fijo de 0x1A2B3C4D. Su propósito es permitir al receptor asegurarse que esta apropiadamente sincronizado con la secuencia de datos TCP.
- Control Message Type: Sus valores pueden ser:

1. Start-Control-Connection-Request
2. Start-Control-Connection-Reply
3. Stop-Control-Connection-Request
4. Stop-Control-Connection-Reply
5. Echo-Request
6. Echo-Reply
7. Outgoing-call-request
8. Outgoing-call-reply
9. Incoming-call-request
10. Incoming-call-reply
11. Incoming-call-connected
12. Call-clear-request
13. Call-Disconnect-Notify
14. Wan-error-notify
15. Set link info

- Reserved: debe ser puesto a 0.

Protocolos de la Capa de Internet

- **Protocolo IP**

En la capa Internet de TCP/IP básicamente existe el protocolo IP (Internet Protocol), IP es independiente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza, sirve como protocolo universal que permite que cualquier computadora en

cualquier parte del mundo pueda comunicarse en cualquier momento, este protocolo es la base fundamental de Internet.
IP que se implementa en software, define las unidades de transferencia de datos (datagramas) y se encarga de su transferencia desde el host origen al host destino, selecciona la trayectoria a seguir por los datagramas, realiza tareas de fragmentación y reensamblado. IP no esta orientado a conexión y no es confiable ya que manda los datagramas sin contar con mecanismos de verificación de entrega y sin comprobación de errores, deja las tareas de control de secuencia, recepción y verificación de datagramas enviados a través de la red a los protocolos de la capa de transporte. El nivel de direccionamiento de TCP/IP se genera aquí, el ruteo o direccionamiento de los datagramas se puede realizar paso a paso por todos los nodos o mediante rutas estáticas o dinámicas.
Los datagramas IP contienen una cabecera con información para el nivel IP y los datos del usuario, estos se encapsulan en tramas de longitud determinada por la red física. Para poder direccionar los datagramas, IP introduce una nueva cabecera en los mismos formada por 160 bits que contienen los datos necesarios para enrutar los paquetes como: la longitud de cabecera del datagrama, numero de identificación, tipo de protocolo al que pertenece el datagrama, campo de comprobación, dirección origen y dirección destino, etc. Al atravesar diferentes redes la longitud puede variar por lo que se establece un tamaño máximo permitido en cada red o MTU (Maximum Transmissión Unit), si el paquete excede este tamaño se debe fragmentar o reensamblar según la dirección de transmisión.
El papel de la capa IP es encaminar datagramas a su destino final, esto lo consigue mediante el protocolo IP, esta es la misión u objetivo principal de esta capa y del protocolo, por lo cual no se preocupa de la integridad de los datos.. Para esto cada interfaz en la red necesita una dirección IP que identifica a cada host de forma única. Dos hosts no pueden tener una misma dirección IP publica, pero si pueden tener la misma IP si pertenecen a dos redes privadas diferentes[2].

- **Protocolo ICMP.**

El protocolo de mensajes de control y error de Internet (Internet Control Message Protocol) es un protocolo de mantenimiento y gestión de la red que ayuda a supervisar la red, así como encontrar la ruta optima de transmisión para los datagramas[2].

- **Protocolo IGMP.**

El protocolo de administración de grupo de Internet IGMP (Internet Group Management Protocol) se usa por los hosts IP para reportar su conjunto de miembros a cualquier router multicast vecino. Es parte integral de IP y debe ser implementado por todos los hosts conformando el nivel 2 de la especificación multicasting IP. Los mensajes IGMP son encapsulados en datagramas IP, con un numero de protocolo IP de 2, el formato del paquete se observa en la Fig. 3.1.1.6.

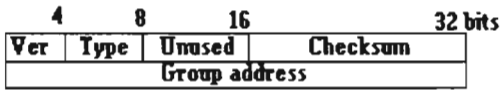


Fig. 3.1.1.6 Paquete IGMP

- Ver: Son 4 bits que indican la versión del protocolo IP. Siempre vale 1.

[2] En los temas siguientes 3.2 y 3.3 se toca mas a fondo este protocolo.

- Type: Tipo de mensaje, especifica que se trata de una consulta o de un informe:
1 Especifica una consulta enviada por un router multicast.
2 Especifica un informe o reporte enviado por un host o el conjunto de miembros host.
- Checksum: Una suma de comprobación de 16 bits calculada de igual forma que con ICMP.
- Group address: En un mensaje de reporte de miembros hosts este campo contiene la dirección de grupo de host IP del grupo que es reportado. Es cero para una solicitud y es una dirección de grupo multicast valida para un informe.

Los mensajes IGMP se envían en datagramas IP. La cabecera IP siempre tendrá un numero de protocolo igual a 2, indicando IGMP y un tipo de servicio cero (rutina). El campo de datos IP contendrá el mensaje IGMP mostrado en la Fig. 3.1.1.6.
El funcionamiento de IGMP es como se describe a continuación:
En IGMP pueden participar hosts y routers multicast.
Los hosts deben unirse a un grupo para recibir mensajes multicast. Un host multipuerto puede unirse a cualquier grupo por una o más de sus interfaces de las redes a las que esta conectado. Los mensajes del mismo grupo en dos subredes distintas son diferentes. 224.0.0.1 es el grupo para todos los hosts de esta subred. Para unirse a un grupo el host envía un informe acerca de una interfaz dirigido al grupo multicast interesado. Los routers multicast de la misma red reciben el informe y activan un flag para indicar que al menos un host de esa red es miembro de ese grupo. Cualquier host pertenece al grupo 224.0.0.1 de forma automática. Los routers multicast tienen que escuchar a todas las direcciones de multicast (todos los grupos) para detectar tales informes. Las alternativas serian el uso de broadcast para los informes o para configurar hosts con direcciones unicast para routers multicast.
Los routers multicast envían regularmente a intervalos de 1 minuto una consulta a la dirección de multicast todos los hosts. Cada host que aun desea ser miembro de uno o más grupos replica una vez por cada grupo en el que este interesado (no al grupo todos los hosts al que pertenece de modo automático). Cada respuesta se envía en intervalos de tiempo aleatorios para evitar aglomeraciones en él trafico A los routers no le importa cuantos hosts son miembros de un grupo y como todos los miembros de ese grupo pueden oír las respuestas de cada uno de los demás hosts, cualquier host que escuche a otro host proclamar su pertenencia al mismo grupo cancelara su respuesta para ahorrar recursos. Si ningún host responde dentro de un intervalo de tiempo dado, el router multicast decide que ningún host pertenece a ese grupo. Cuando un host o router multicast recibe un datagrama multicast, su acción depende del valor TTL y de la dirección IP de destino:
0 Un datagrama enviado con un TTL=0 se restringe al host emisor.
1 Un datagrama con TLL=1 alcanza todos los hosts de la subred que son miembros del grupo. Los routers multicast decrementan el TTL a cero pero a diferencia del datagrama unicast no lo informan con un mensaje ICMP (time exceded). La expiración de un datagrama multicast es un evento normal.
2+ Todos los hosts miembros del grupo y todos los routers multicast reciben el datagrama. La acción de los routers depende de la dirección de grupo multicast.
224.0.0.0-224.0.0.255 Este rango se emplea solo apara aplicaciones multicast que hagan uso de un único salto. Los routers multicast no retransmitirán datagramas con direcciones IP en este rango. El informe de la pertenencia a este grupo indica a otros hosts de la subred

que el host informante es miembro del grupo. El único miembro del que nunca se da parte es el 224.0.0.1.
other El router retransmite los datagramas con otros valores para la dirección de destino: El valor TTL sé decrementara en al menos un segundo. Esto permite a un host localizar al servidor más cercano que este escuchando sobre una dirección multicast usando una búsqueda expansiva en anillo. El host envía un datagrama con un valor TTL de 1 (misma subred) y espera una respuesta. Si no se recibe respuesta prueba con un TTL de 2, de 3, etc. al encontrar al servidor más cercano.

Protocolos para actualización automática de la tabla de direccionamiento (ruteo).
TCP/IP contiene un conjunto de protocolos que son usados por el nivel de Internet para actualizar las tablas de ruteo de los dispositivos que funcionan en este nivel (routers). Estos protocolos de ruteo se clasifican en:

- Protocolos de ruteo interior IGP (Interior Gateway Protocol). Son los protocolos usados para realizar la función de ruteo dentro de un dominio o sistema autónomo.
- Protocolos de ruteo exterior EGP (Exterior Gateway Protocol). Son los protocolos usados para realizar la función de ruteo entre dominios o sistemas autónomos.

- Protocolos de ruteo interior IGP.

Los protocolos de ruteo interior a su vez se subdividen por el tipo de algoritmo para determinación de ruta en:

- Protocolos de vector distancia. Los protocolos que usan este algoritmo son RIPv1 e IGRP.
- Protocolos de estado de enlace. Estos protocolos son OSPF e IS-IS.
- Protocolos híbridos. Los protocolos híbridos que usan un balance híbrido empelan técnicas de ambos algoritmos de vector distancia y estado de enlace son RIPv2 y EIGRP.

- Protocolos de ruteo exterior EGP.

Dentro de los protocolos de ruteo exterior básicamente se encuentran:

- BGPv4. Este es el protocolo de ruteo exterior usado extensivamente en Internet.
- IDRP.

La Fig. 3.1.1.7 nos muestra un esquema de los protocolos de ruteo[3].

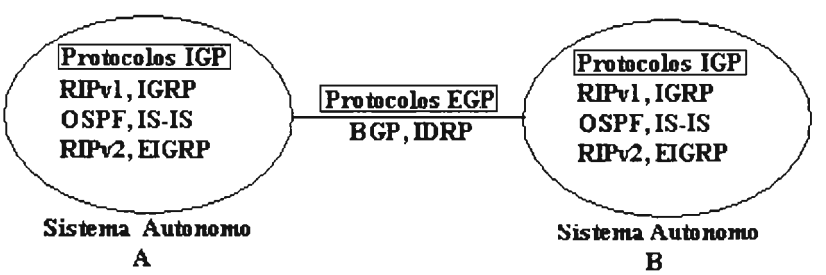


Fig.3.1.1.7 Protocolos de ruteo

[3] Los protocolos seran revisados en el tema 3.3.6

- **Protocolo de seguridad AH**

El protocolo de autenticación del encabezado IP busca proporcionar seguridad agregando información de autentificación a un datagrama IP. La información de autentificación es calculada usando todos los campos en el datagrama IP (incluidos no solo el encabezado IP sino también otros encabezados y datos de usuarios) que no cambian en él transito. Los campos u opciones que necesitan cambiar en transito (como cuenta de saltos, tiempo de vida, ident, fragment, offset o apuntador de ruteo) son considerados como cero para el calculo de los datos de autentificación. Esto proporciona mas seguridad que la actualmente presente en IPv4 y puede ser suficiente para las necesidades de muchos usuarios. Cuando es usado con IPv6 el encabezado de autentificación normalmente aparece después del encabezado hop by hop de IPv6 y antes de las opciones de destino IPv6. Cuando es usado con IPv4, el encabezado de autentificación normalmente sigue al encabezado IPv4 principal. El numero de protocolo asignado a AH es el 49. Este formato se muestra en la Fig. 3.1.1.8.

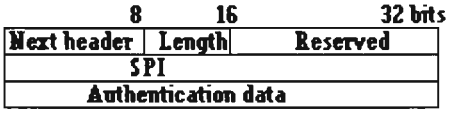


Fig. 3.1.1.8 Formato del paquete del encabezado AH

- Next header: La siguiente carga útil después de la carga útil de autentificación
- Length: La longitud del campo de datos de autentificación.
- Reserved: puesto a cero.
- Security Parameter Index (SPI): Identifica la asociación de seguridad para este datagrama.
- Authentication data: Numero variable de palabras de 32 bits.

- **Protocolo de seguridad ESP.**

El protocolo ESP (Encapsulated Security Payload) IP busca proporcionar confidencialidad e integridad encriptando los datos a ser protegidos y colocando los datos encriptados en la porción de datos del IP ESP. Dependiendo de los requerimientos de seguridad del usuario puede ser usado para encriptar ya sea un segmento de la capa de transporte (TCP, UDP, ICMP, IGMP, etc.) o un datagrama entero IP. Encapsular el dato protegido es necesario para proporcionar confidencialidad al datagrama original entero.

ESP puede aparecer en cualquier lugar después del encabezado IP y antes del final del protocolo de la capa de transporte. El IANA ha asignado el protocolo numero 50 a ESP. El encabezado inmediatamente precediendo un encabezado ESP siempre contendrá el valor 50 en su campo Next Header (IPv6) o Protocol (IPv4). ESP consiste de un encabezado no encriptado seguido por datos encriptados. Los datos encriptados incluyen tanto el campo del encabezado ESP protegido y los datos de usuario protegidos, el cual es ya sea un datagrama IP entero o una trama de protocolo de capa superior (TCP, UDP). El formato del encabezado se observa en la Fig. 3.1.1.9.

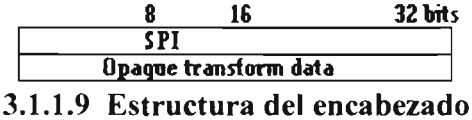


Fig. 3.1.1.9 Estructura del encabezado ESP

- Security parameter index (SPI): Es un valor pseudo aleatorio de 32 bits que identifica la asociación de seguridad para este datagrama. Si no se ha establecido una asociación de seguridad, el valor del campo es 0x00000000. El SPI es similar al SAID usado en otros protocolos de seguridad.
- Opaque transform data: Campo de datos de longitud variable.

- **Protocolo ISAKMP**

El protocolo de administración de llave y asociación de seguridad de Internet ISAKMP (Internet Security Association Key Management Protocol) define procedimientos y formatos de paquete para establecer, negociar, modificar y borrar asociaciones de seguridad (AS). Las AS contienen toda la información requerida para la ejecución de varios servicios de seguridad de red, tal como los servicios de capa IP (autentificación de encabezado y encapsulación de la carga útil), servicios de transporte o de la capa de aplicación, o autoprotección de la negociación de trafico. Define las cargas útiles para el intercambio de llave de generación y autentificación de datos. Estos formatos proporcionan un armazón consistente para la transferencia de llaves y autentificación de datos, lo cual es independiente de la técnica de generación de llave, algoritmo de encripción y mecanismo de autentificación. El formato del encabezado se muestra en la Fig. 3.1.1.10.

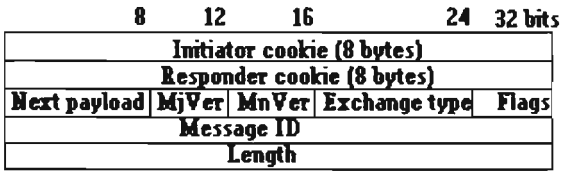


Fig. 3.1.1.10 Encabezado ISAKMP

- Initiator cookie: Cookie de la entidad que inicio el establecimiento de la AS, notificación de la AS, o borrado de la AS.
- Responder cookie: Cookie de la entidad que esta respondiendo a un establecimiento de la AS, notificación de la AS, o borrado de la AS.
- Next payload: Indica el tipo de la primer carga útil en el mensaje. Los posibles tipos son:

0 ninguno
1 Asociación de seguridad (SA)
2 Propuesta (P)
3 Transform (T)
4 Intercambio de llave (KE)
5 Identifiacación (ID)
6 Certificado (CERT)
7 Petición de certificado (CR)
8 Hash (HASH)
9 Firma (SIG)
10 Nonce (NONCE)
11 Notificación (N)
12 Borrar (D)
13 Identificador del vendedor (VID)
14-127 Reservado

128-255 Uso privado

- Mver: Indica la versión mayor del protocolo ISAKMP en uso. Las implementaciones basadas en el RFC 2408 deben establecer la versión mayor a 1. Las implementaciones basadas en versiones previas de proyectos de Internet ISAKMP deben establecer la versión mayor a 0. Las implementaciones nunca deberán aceptar paquetes con un numero de versión mayor más grande que la propia.
- MnVer: Indica la versión menor del protocolo ISAKMP en uso. Las implementaciones basadas en el RFC 2408 deben establecer la versión menor a 0. Las implementaciones basadas en versiones previas de proyectos de Internet ISAKMP deben establecer la versión menor a 1. Las implementaciones nunca deberán aceptar paquetes con un numero de versión menor más grande que la propia.
- Exchange type: Tipo de intercambio a ser usado. Divide los mensajes y clasificación de carga útil en los intercambios ISAKMP. Los posibles valores son:

0 Ninguno
1 Base
2 Protección de identidad
3 Solamente autentificación
4 Agresivo
5 Informacional
6-31 Uso futuro ISAKMP
32-239 Uso especifico DOI
240-255 Uso privado.

- Flags: Opciones especificas que son establecidas por el intercambio ISAKMP.

E(ncryption) (bit 0)- especifica que todas las cargas útiles siguientes al encabezado son encriptadas usando el algoritmo de encriptamiento identificado en el ISAKMP SA.
C(ommit) (bit 1)-Señaliza la sincronización del intercambio de llaves. Es usada para asegurarse que el material encriptado no es recibido antes de la realización del establecimiento de la AS.
A(uthentication only bit) (bit 2): Pretensión de uso con el intercambio informacional con una notificación de carga útil y permitirá la transmisión de información con el chequeo de integridad pero sin encripción. Los bits restantes son puestos a 0 antes de la transmisión.
Message ID: Identificador de mensaje único usado para identificar el estado del protocolo durante la fase 2 de las negociaciones. Este valor es aleatoriamente generado por el iniciador de la negociación de la fase 2. En el caso de establecimiento de SA simultaneas (colisiones) el valor de este campo parecerá ser diferente por que son independientemente generados y así dos asociaciones de seguridad progresaran hacia el establecimiento. Sin embargo indistintamente habrá establecimientos simultáneos. Durante las negociaciones de fase 1 el valor debe ser puesto a 0.

- Length: Longitud del mensaje total (encabezado +carga útil) en octetos. La encripción puede expandir el tamaño de un mensaje ISAKMP.

Protocolos de Capa de transporte

- **Protocolo TCP**

El protocolo de control de transmisión TCP (Transmission Control Protocol) es un protocolo confiable orientado a conexión (establece una conexión lógica entre procesos pares) que utiliza los servicios del nivel de red o Internet para transferencias de largas cantidades de datos de una sola vez. Ofrece de manera flexible y alta calidad comunicaciones confiables sin problemas de flujo y con recuperación de errores. La confiabilidad del protocolo se basa en la correcta entrega de los paquetes mediante el uso de números de secuencia y reconocimientos (ACK=acknowledgements) de mensajes recibidos. Los números de secuencia permiten que los mensajes grandes sean segmentados y reensamblados en el origen y destino cuando la red lo requiera. El reconocimiento verifica que la información haya sido recibida.

Por ser un protocolo orientado a conexión, atiende a los servicios de la capa de aplicación orientados a conexión. Los servicios que suministra a las aplicaciones son:

- Servicio orientado a conexión.

El servicio de entrega de flujo en la maquina destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en la maquina origen.

- Conexión de circuito virtual

El software de protocolo se comunica continuamente durante al transferencia para verificar que los datos se reciban correctamente, si la comunicación falla ambas maquinas detectan la falla y la reportan a los programas de aplicación.

- Transferencia de datos a través de un canal

TCP trasfiere un flujo continuo de bytes a través de Internet, la aplicación no se preocupa de trozar los datos en bloques o datagramas, ya que TCP se encarga de ello al agrupar los datos en segmentos, decidiendo como segmentarlos y puede enviarlos del modo que más le convenga

- Confiabilidad.

Durante la transferencia el software de protocolo en las dos maquinas continua comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo, ambas maquinas detectaran la falla y la reportaran a los programas de aplicación.

TCP asigna un numero de secuencia a cada byte transmitido y espera un reconocimiento afirmativo (ACK) del TCP receptor, si el ACK no se recibe en un intervalo de timeout los datos se retransmiten. El TCP receptor usa los números de secuencia para organizar los segmentos cuando llegan fuera de orden, así como para eliminar segmentos duplicados. La confiabilidad que se proporciona depende del servicio de entrega de flujo.

- Control de flujo.

El TCP receptor regresa junto con el ACK él numero de bytes que puede recibir aun sin que se produzca sobrecarga y desbordamiento de sus buffers internos. Este valor se envía en el ACK en la forma del numero de secuencia mas elevado que se puede recibir sin problemas. Este es el mecanismo de ventanas.

- Transferencia con memoria intermedia.

Las aplicaciones envían un flujo de datos a través del circuito virtual pasando bytes al software de protocolo, cada aplicación usa piezas del tamaño que encuentre adecuado que pueden ser del tamaño de un byte. En el receptor el software de protocolo entrega los bytes

del flujo de datos en el mismo orden recibido a la aplicación tan pronto como se reciben y verifican. Para hacer eficiente la transferencia y minimizar él trafico de red por lo general se recolectan los suficientes datos de un flujo para llenar un datagrama lo suficientemente largo antes de enviarlo.

- Multiplexación

Se implementa usando puertos de conexión.

- Conexiones lógicas.

Para mantener la fiabilidad y control de flujo TCP requiere cierta información de estado para cada canal. Este estado junto con los sockets, números de secuencia y tamaños de ventanas forman la conexión lógica que se define por el par del socket del emisor y el receptor.

- Full duplex.

TCP permite la concurrencia de los flujos de datos en ambos sentidos de la conexión, estos flujos son independientes y sin ninguna interacción entre sí, las conexiones full duplex permiten la existencia de flujos independientes en direcciones opuestas.. Así el software subyacente de protocolo puede enviar datagramas de información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga reduce él trafico en la red.

- Flujo no estructurado: Se puede enviar información de control junto a los datos.
- Es un protocolo confiable implementado con: el uso de checksum confirmación de recepción, temporizadores de espera de confirmación y retransmisión de segmentos por que permite la recuperación de datos perdidos o duplicados y garantiza la secuencia de entrega asignando un numero de secuencia.
- La unidad de datos que maneja TCP se conoce como segmento

El principio de ventana.

Un protocolo de transporte simple usa el principio de: enviar un paquete, esperar un ACK del receptor antes de enviar el siguiente, Fig. 3.1.1.11 a). Si el ACK no se recibe dentro de cierto tiempo, se retransmite Fig. 3.1.1.11 b).

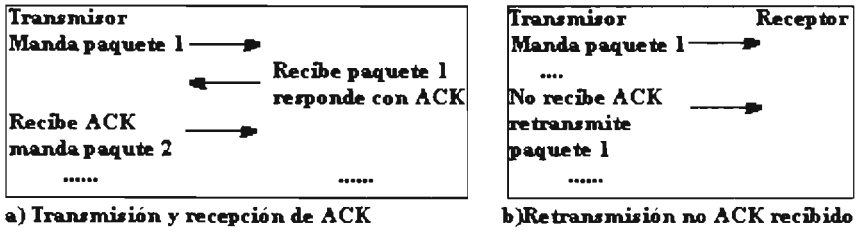


Fig. 3.1.1.11 Transmisión de paquetes con recepción/sin recepción de ACK

Este mecanismo es confiable pero solo usa una parte del ancho de banda de la red. Ahora si un emisor agrupa paquetes como muestra la Fig. 3.1.1.12

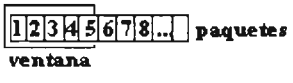


Fig. 3.1.1.12 Paquetes del mensaje

Y usa las siguientes reglas:

- El emisor puede enviar todos los paquetes dentro de la ventana sin recibir un ACK, pero dispara un cronometro para el timeout de cada uno.
- El receptor debe reconocer cada paquete recibido indicando él numero de secuencia del ultimo paquete bien recibido.
- El emisor desliza la ventana para cada ACK recibido.

En el caso mostrado en la Fig. 3.1.1.13, el emisor puede transmitir los paquetes del 1 al 5 sin recibir respuesta.

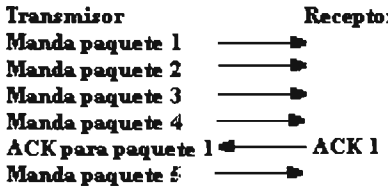


Fig.3.1.1.13 Principio del ventaneo

Cuando el emisor recibe el ACK 1 puede deslizar su ventana para excluir el paquete 1 y ya puede transmitir el paquete 6. Si se da el caso de que un paquete no se reciba en el receptor, el emisor no recibirá el ACK de ese paquete y lo tendrá que retransmitir, si es el ACK el que no reciba el emisor, al recibir el ACK del siguiente paquete sabrá que el paquete anterior si fue recibido por lo que puede deslizar su ventana al siguiente paquete. Por lo tanto el mecanismo de ventanas asegura:

- Una transmisión confiable
- Mejor aprovechamiento del ancho de banda
- Control de flujo ya que el receptor puede retrasar la respuesta a un paquete con un reconocimiento, conociendo los buffers libres de los que dispone y el tamaño de la ventana de comunicación.

El mecanismo de ventanas se usa en TCP con algunas diferencias:

- Los números de secuencia se aplican a cada byte del canal. TCP divide el flujo de bytes en segmentos. El principio de la ventana se aplica a nivel de bytes, los segmentos enviados y los ACKs recibidos llevaran números de secuencia de forma que el tamaño de la ventana se exprese con un numero de bytes, en vez del de paquetes.

El tamaño de la ventana lo determina el receptor, cuando se establece la conexión y puede variar durante la transmisión de datos. Cada ACK incluirá el tamaño de la ventana que acepta el receptor en ese momento.

TCP agrupa los bytes en segmentos, y un segmento TCP solo lleva él numero de secuencia del primer byte.

Para calcular el timeout TCP registra el momento de envío de un segmento y el de recepción de un ACK, se promedia un valor para varios de estos viajes y será el valor del timeout del siguiente segmento a enviar.

Establecimiento de una conexión TCP

En TCP antes de transmitir cualquier dato se establece una conexión entre dos procesos, Fig. 3.1.1.14.

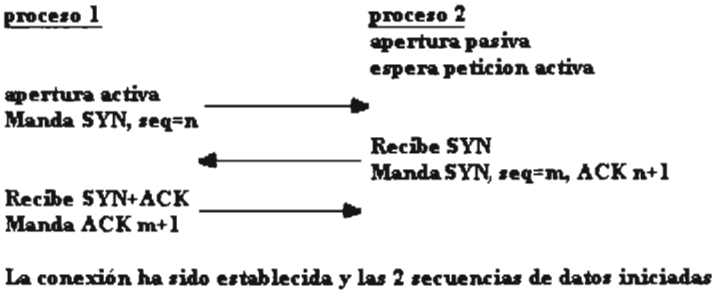


Fig. 3.1.1.14 Establecimiento de conexión TCP

Se intercambian tres segmentos TCP conocidos como three-way handshake o acuerdo en 3 fases, una apertura pasiva permanece en espera hasta que un proceso se comunica a través de una apertura activa. Los segmentos TCP intercambiados incluyen los números de secuencia iniciales de ambas partes, para ser usados en posteriores transferencias. El cierre de la conexión se realiza enviando un segmento TCP con el bit fin activo, el segmento de cierre se manda en ambos sentidos. Por lo tanto TCP realiza la transmisión en tres fases:

- Establece la conexión y él numero de secuencia inicial.
- Transfiere la información por segmentos agregando un encabezado con él numero de secuencia y un código de control. La confiabilidad de este protocolo se basa con la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.
- Finaliza la conexión.

El inicio, mantenimiento y cierre de una conexión requiere que el TCP recuerde toda la información relativa a cada conexión. Algunos estados del TCP son:

0. Closed: No existe, solo para referencia.
1. Listen: Esperando solicitud de conexión de un TCP remoto.
2. SYN-SEN: Esperando un mensaje de solicitud de conexión después de haber enviado una solicitud de conexión.
3. SYN-RECEIVED: Esperando confirmación de un reconocimiento de solicitud de conexión, después de haber enviado y recibido una solicitud de conexión.
4. ESTABLISHED: Representa una conexión abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este es el estado normal de la fase de transferencia de la conexión.
5. FIN-Wait-1: Esperando la solicitud de fin de conexión de un TCP remoto, o un reconocimiento de una solicitud de fin de transmisión enviada anteriormente.
6. FIN-WAIT-2: Esperando una solicitud de fin de conexión de un TCP remoto.
7. CLOSE-WAIT: Esperando una solicitud de fin de conexión de un protocolo de una capa superior.
8. CLOSING: Esperando el conocimiento de una solicitud de final de conexión enviada anteriormente al TCP remoto.
9. TIME-WAIT: Esperando el tiempo necesario para que el TCP remoto haya recibido el conocimiento de la solicitud del fin de conexión.

Este protocolo permite la multiplexación por lo que una conexión puede ser usada por varios usuarios simultáneamente. Para esto define puertos para cada aplicación o usuario. Un puerto es una palabra de 16 bits que identifica las aplicaciones o procesos de TCP/IP. Los puertos se clasifican en el RFC 1700 en tres rangos:

- Puertos bien conocidos que van desde el 0 hasta el 1023 son asignados por el IANA y en la mayor parte de sistemas solo pueden ser usados por procesos de sistema o programas ejecutados por usuarios privilegiados. Estos puertos son usados en TCP para identificar las puntas de conexiones lógicas que transportan conversaciones. Un puerto de contacto de servicio es definido para proporcionar servicios a usuarios desconocidos, estos puertos de contacto son los puertos bien conocidos. Algunos de los mas usados se listan en la tabla 3.1.1.2.

Nombre o clave	Puerto/protocolo de transporte	Descripción
echo	7/tcp/udp	Echo
ftp-datos	20/tcp/udp	Transferencia de archivos (Datos)
ftp-control	21/tcp/udp	Trasferencia de archivos (Control)
ssh	22/tcp/udp	SSH remoto
telnet	23/tcp/udp	Telnet
smtp	25/tcp/udp	Simple Mail Transfer
tacacs	49/tcp/udp	Login host protocol (TACACS)
domain	53/tcp/udp	Domain Name Server
tacacs-ds	65/tcp/udp	TACACS-Database Service
sql*net	66/tcp/udp	Oracle SQL-Net
bootps	67/tcp/udp	Bootstrap Protocol Server
bootpc	68/tcp/udp	Bootstrap Protocl client
tftp	69/tcp/udp	Trivial File Transfer
http	80/tcp/udp	World Wide Web HTTP
kerberos	88/tcp/udp	Kerberos
pop3	110/tcp/udp	Post Office Protocol Version 3
auth	113/tcp/udp	Authentication Service
sqlserv	118/tcp/udp	SQL Services
ntp	123/tcp/udp	Network Time Protocol
netbios-ns	137/tcp/udp	NETBIOS Name Service
netbios-dgm	138/tcp/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp/udp	NETBIOS Session Service
snmp	161/tcp/udp	SNMP
snmptrap	162/tcp/udp	SNMPTRAP
bgp	179/tcp/udp	Border Gateway Protocol
irc	194/tcp/udp	Internet Relay Chat Protocol
ipx	213/tcp/udp	IPX
http-mgmt	280/tcp/udp	Http-mgmt
https	443/tcp/udp	Http protocol over TLS/SSL

exec	512/tcp	Remote process execution; autentificación usando passwords y nombres de comienzo de sesión en UNIX
router	520/udp	Proceso de ruteo local
ripng	521/tcp/udp	Ripng
irc-serv	529/tcp/udp	IRC-SERV
rpc conference	531/tcp/udp	Chat conference
dhcpv6-client	546/tcp/udp	DHCPv6 Client
dhcpv6-server	547/tcp/udp	DHCPv6 Server
syslog-conn	601/tcp/udp	Reliable Syslog Service
sshell	614/tcp/udp	SSLshell
ftps-data	989/tcp/udp	ftp protocol, daos sobre TLS/SSL
ftps	990/tcp/udp	ftp protocol, control SSL/TLS
telnets	992/tcp/udp	telnet protocol sobre TLS/SSL
Ircs	994/tcp/udp	Irc protocl over TLS/SSL
Pop3s	995/tcp/udp	Pop3 over TLS/SSL

Tabla 3.1.1.2 Puertos bien conocidos

- Puertos registrados que van desde el 1024 hasta el 49151 son listados por IANA y en la mayoría de los sistemas pueden ser usados por procesos de usuario ordinario o programas ejecutados por usuarios ordinarios, los puertos son usados por TCP para nombrar las puntas de las conexiones lógicas que transporta las conversaciones. Para proporcionar servicios a usuarios desconocidos, un puerto de contacto de servicio es definido. La lista especifica tanto el puerto usado por el proceso servidor como su puerto de contacto. El IANA registra los usos de estos puertos como una conveniencia a la comunidad. Donde se dé el caso, las mismas asignaciones de puerto son usadas con UDP.
- Puertos privados y/o dinámicos que van desde 49152 hasta el 65535.

De esta forma los servidores asignaran a cada servicio un puerto por el que estarán escuchando las peticiones de conexión y por el que podrán diferenciar las peticiones que intentan conectarse a algún servicio como muestra la Fig. 3.1.1.15.

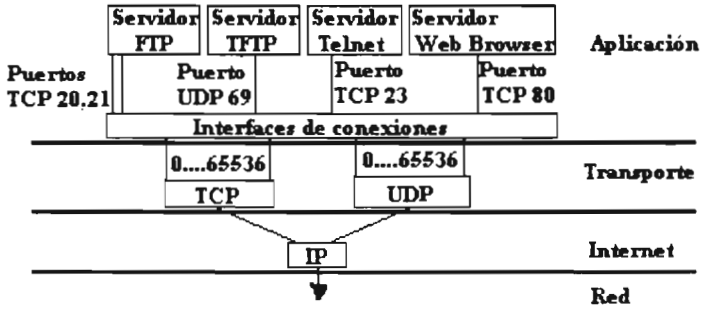


Fig. 3.1.1.15 Puertos y conexiones

Sockets

En TCP dos procesos se comunican a través de sockets TCP. El socket proporciona a un proceso una conexión con un flujo full duplex de bytes con otro proceso. La aplicación no necesita preocuparse de la gestión de este canal, esto lo hace TCP. TCP usa puertos efímeros y bien conocidos.

Para realizar una conexión con TCP el cliente hace una solicitud de servicios al servidor mediante el uso de sockets. El servidor y el receptor deben crear los sockects o puntos terminales de conexión. Los dos campos del socket son:

- La dirección IP del host en que la aplicación esta corriendo.
- El puerto de protocolo a través del cual la aplicación se comunica con TCP/IP, este es un numero de 16 bits que es de carácter local al host. Por lo tanto tenemos la asociación:

Socket=TCP+Dirección IP+Puerto de Protocolo.

El socket local se construye concatenando la dirección IP de origen y él numero de puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y el numero de puerto de destino. Si dos procesos se comunican sobre TCP tendrán una conexión lógica identificable unívocamente por medio de los sockets implicados es decir la combinación <TCP, dirección IP local, puerto local, dirección IP remota, puerto remoto>.

El numero de puerto será uno de los listados en la tabla 3.1.1.2 que son publicados por IANA, esto cuando son los puertos comunes que se usan para permitir el acceso a los servicios, pero también puede usarse puertos modificados por el usuario para implementar cierta seguridad, por ejemplo en lugar de usar el puerto 23 de telnet se puede definir que el protocolo use el puerto 2323. Por su parte el cliente quien es el que hace la solicitud utiliza cualquier puerto libre que él tenga, por lo tanto una conexión será definida por dos puntos extremos (sockets), Fig. 3.1.1.16.

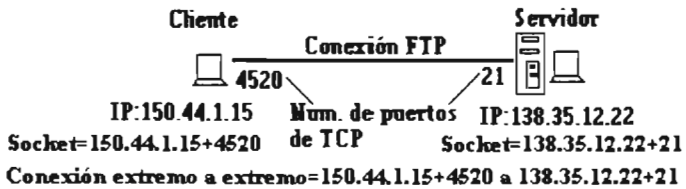


Fig. 3.1.1.16 Conexión o socket de TCP

Los procesos del servidor son capaces de gestionar múltiples conversaciones a través de un único puerto a través de la multiplexación que permite la conexión de varios clientes al mismo tiempo, para esto hace uso de los sockets en los cuales él numero de puerto a que se conectan los clientes es siempre el mismo, diferenciándose las múltiples conexiones por la dirección IP del cliente y el puerto que se uso para establecer la conexión. Fig. 3.1.1.17.

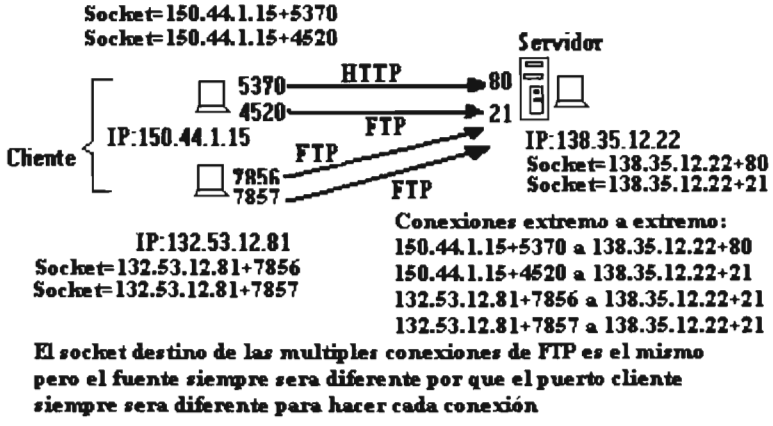


Fig. 3.1.1.17 Conexión de varios clientes con TCP

En conexiones múltiples cada una esta identificada por una pareja IP-Puerto de forma única.

Para establecer conexiones entre dos hosts el extremo servidor debe realizar una apertura pasiva del puerto, es decir, dejarlo abierto para escuchar las peticiones de conexión, el extremo cliente debe realizar una apertura activa en el puerto servidor, abriendo un puerto propio y conectándose con el puerto que escucha en el servidor. Generalmente los servidores dejan abiertos sus puertos conocidos mientras que un programa o demonio permanece a la espera de peticiones de conexión. Tanto TCP como UDP usan números de puerto para enviar información a las capas superiores.

Los segmentos TCP que se transmiten de extremo a extremo tienen un formato, Fig. 3.1.1.18, cada segmento esta dividido en dos partes: una cabecera seguida de datos. La cabecera TCP contiene la información de identificación y control.

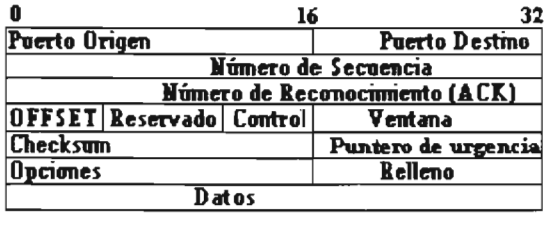


Fig. 3.1.1.18 Formato de los segmentos TCP

Los campos de la cabecera del segmento TCP son:

- Puerto origen. Puerto a través del cual una aplicación invoca a TCP y a través del cual el receptor responde, su longitud es de 16 bits.
- Puerto destino. Es el puerto de la aplicación destino, su tamaño es de 16 bits
- Número de secuencia. Es el número de secuencia del primer byte de datos enviado en este segmento. Si el byte de control SYN esta a 1, el numero de secuencia es el inicial (n) y el primer byte de datos será el n+1.
- Numero de reconocimiento. Si el bit de control esta a 1 este campo contiene el numero de secuencia del primer byte del segmento que se espera recibir.

- OFFSET. Es un numero entero que especifica la longitud de la cabecera en múltiplos de 32 bits. Su longitud es de 4 bits. Indica donde empiezan los datos.
- Reservado. Campo de 6 bits reservado para uso futuro, deben ser cero.
- Control. Campo de 6 bits de longitud donde cada bit indica el tipo de segmento, es decir indica como deben interpretarse algunos campos de la cabecera:
  - URG: Si el primer bit es 1 este segmento es urgente
  - ACK: El segundo bit indica que el segmento es de confirmación.
  - PSH: Cuando el receptor recibe un segmento con el tercer bit (PUSH) activado debe enviar los datos que almaceno en su buffer l proceso del cual acaba de recibir el segmento de PUSH.
  - RST: Con el cuarto bit activado el segmento resetea la conexión.
  - SYN: Si el bit cinco esta en 1 este segmento sincroniza el numero de secuencia.
  - FIN: Con el bit seis encendido se indica que ya no hay mas datos para el receptor.
- Ventana: Indica el tamaño del buffer disponible que tiene el emisor para recibir datos. Este campo permite a TCP implementar el control de flujo puesto que indica el numero máximo de octetos que pueden ser recibidos. El receptor de un segmento con el campo window a cero no puede enviar mensajes al emisor, excepto mensajes de prueba. Un mensaje de prueba es un mensaje de un solo octeto que se utiliza para detectar redes o hosts inalcanzables.
- Checksum: Este campo es el complemento a 1 de 16 bits de la suma de los complementos a 1 de todas las palabras de 16 bits de la pseudocabecera, cabecera TCP y los datos TCP. La pseudocabecera es una pseudocabecera IP usada solo para calcular el checksum.
- Puntero urgente: Cuando este puntero se activa es por que los datos son urgentes por lo que el programa TCP debe procesarlos de inmediato y posteriormente volver al modo normal, el bit urgente señala la posición en la ventana donde los datos urgentes acaban. Cuando esto sucede los datos se envían fuera de banda y se envían sin esperar sin esperar a que el programa este listo para recibir datos. Solo es significativo cuando el bit URG esta a uno.
- Opciones. Se indica el tamaño máximo del segmento. Esta opción solo es valida durante el establecimiento de la conexión (bit de control SYN puesto a 1) y se envía desde el extremo que ha de recibir datos para indicar la máxima longitud de segmento que es capaz de manejar. Si esta opción no se usa se admiten segmentos de cualquier tamaño.
- Relleno. Son bits a cero que se utilizan para rellenar la cabecera TCP de manera que esta alcance una longitud total que sea múltiplo de 32.

TCP es el protocolo de propósito general para la transferencia de grandes volúmenes de información, ya que en el nivel mas bajo, o sea IP, las redes de comunicación proporcionan una entrega de paquetes no confiable, pero los paquetes se pueden destruir por errores de falla de hardware, congestión de la red, o debido a que en las redes que rutean los paquetes estos pueden llegar en desorden, con retraso o duplicados, es en estos casos que los programas de aplicación hacen uso de TCP para asegurar la correcta entrega de esas grandes cantidades de información.

Algunas aplicaciones estándar que usan TCP son: FTP, Telnet, HTTP, DNS, SMTP, POP, X-WINDOW.

- **Protocolo UDP**

El protocolo del nivel de transporte para el intercambio de datagramas de usuario (UDP) es un protocolo no orientado a conexión ya que el datagrama incorpora la suficiente información de direccionamiento, no es confiable puesto que no garantiza la entrega de paquetes ya que no maneja reconocimientos (acknowledgements), la aplicación es la que se encarga del control de la integridad. Transmite los datos sin establecer una conexión previa, por lo que no se tiene la certeza de que los datagramas lleguen a su destino. Hace uso del protocolo IP para transportar o rutear los datagramas entre las maquinas los cuales deben llevar la dirección completa del destino agregándole la capacidad de distinguir entre varios destinos. Para IP, UDP es solo un interfaz de aplicación que no añade fiabilidad, control de flujo o recuperación de errores a IP, simplemente sirve como multiplexor demultiplexor para enviar datagramas, usando puertos para dirigir los datagramas.

Las aplicaciones que envían datagramas a un host necesitan identificar algo mas que la dirección IP, ya que los datagramas se dirigen a procesos concretos y no a todo el sistema, UDP permite hacer esto con el uso de los puertos. Para esto proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma maquina, agrega los puertos de origen y destino en cada mensaje UDP con los cuales el software UDP en el destino entrega el mensaje al receptor correcto. Un puerto es un numero de 16 bits que identifica en un host que proceso esta asociado a un datagrama. Hay dos tipos de puerto:

Bien conocidos (well-known): Pertenecen a servidores estándar como Telnet usa el puerto 23. Estos se encuentran en el rango de 1 a 1023[4]. La razón de ser de los puertos bien conocidos es permitir a los clientes encontrar a los servidores sin necesidad de información de configuración.

Efímeros: Los clientes no necesitan puertos bien conocidos por que inician la comunicación con los servidores y los datagramas UDP enviados al servidor contienen su numero de puerto. El host en funcionamiento proporciona un puerto a cada proceso cliente mientras lo necesite. Los números de puerto efímeros tienen valores mayores a 1023, por lo general en el rango de 1024 a 5000. Un cliente puede usar cualquier numero en este rango siempre que la combinación <protocolo de transporte, dirección IP, numero de puerto> sea univoca.

La dirección IP sirve para dirigir el datagrama hacia una maquina en particular, y el numero de puerto destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso especifico. La cabecera también contiene el numero de puerto origen que permite al proceso recibido conocer como responder al datagrama.

Cada datagrama UDP se envía en un datagrama IP. Los mensajes UDP se componen de un encabezado UDP de 16 bytes y un área de datos UDP. Fig. 3.1.1.19.

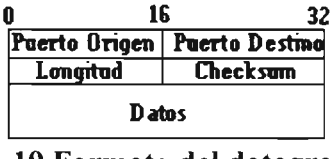


Fig. 3.1.1.19 Formato del datagrama UDP

El encabezado se divide en 4 campos de 16 bits que especifican:

- Puerto origen. Puerto del proceso emisor al que se deben dirigir las respuestas. El campo es de 16 bits.

[4] Consultar tabla 3.1.1.4

- Puerto destino. Puerto del proceso destino en el host destino. También es de 16 bits.
- Longitud. Longitud en bytes del datagrama UDP incluyendo la cabecera.
- Checksum. El complemento a 1 de 16 bits de la suma en complemento a 1 de una pseudocabecera IP, la cabecera UDP y los datos UDP.

Las características de UDP son:
- Entrega de datagramas sin conexión y sin confiabilidad.
- No emplea acuses de recibo.
- No ordena los mensajes entrantes.
- No hay control de la velocidad de flujo de información entre las maquinas. Los mensajes se pueden perder, duplica o llegar sin orden, o llegar mas rapido al receptor de lo que este puede procesarlos.
- Maneja puertos y sockets para realizar la nultiplexión, reconexiones simultáneas de varias aplicaciones.

La multiplexión y demultiplexión entre el software de UDP y los programas de aplicación se realiza mediante puertos. Cada programa de aplicación negocia con el sistema operativo para obtener un puerto de protocolo y un numero de puerto antes de enviar datagramas UDP. Una vez asignado el puerto cualquier datagrama que envíe la aplicación pondrá el numero en el campo de numero de puerto UDP.
UDP no emplea acuses de recibo para asegurarse de que llegan mensajes. No ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las maquinas. Por lo tanto los mensajes de UDP se pueden perder, duplicar o llegar sin orden, además de que pueden llegar más rápido de lo que el receptor los puede procesar.
Algunas aplicaciones estándar que usan UDP son: TFTP, DNS, RPC usado por el NFS, NCS, SNMP, Ping, Traceroute, BOOTP, DHCP.

Protocolos de aplicación

El nivel de aplicación de TCP/IP permite la máxima flexibilidad para los desarrolladores de software.
Todas las aplicaciones TCP/IP se basan en el modelo cliente-servidor. Muchas de estas aplicaciones usan las llamadas de procedimiento remoto RPC (Remote Procedure Call). Una RPC es una llamada a un procedimiento que se ejecuta en un sistema diferente del que se realiza la llamada, representa uno de los procedimientos usados para la realización de aplicaciones distribuidas. En una RPC el programa que realiza la llamada y el procedimiento llamado se comunican a través de una interfaz RPC que se forma por las operaciones y datos que sirven de contrato para un conjunto de procedimientos remotos. El cliente envía un mensaje al proceso servidor y espera una respuesta, el servidor que se encuentra en espera de peticiones al recibir el mensaje del cliente estudia los parámetros del procedimiento llamado, obtiene los resultados y los envía de vuelta mediante una respuesta al cliente.
Algunos de los servicios de aplicación más usados son los siguientes:

❖ **Aplicaciones o utilerías de diagnostico.**

- **PING**

El PING (Packet Internet Groper) es una de las aplicaciones o utilerías más sencillas de TCP/IP verifica los protocolos y los medios físicos, envía uno o más datagramas a un host de destino determinado solicitando una respuesta y mide el tiempo que tarda en retornar.

Este es una de las primeras pruebas para comprobar si es posible alcanzar un host, aunque actualmente con el uso de firewalls la prueba con el ping no es determinante ya que anteriormente si se alcanzaba un host con ping se podía realizar un telnet o ftp, actualmente los firewalls pueden permitir el ping pero cierran el protocolo de aplicación y/o numero de puerto de otra aplicación. Ping usa los mensajes Echo (8) y Echo reply (0) de ICMP. La sintaxis del ping varia según la plataforma donde se aplique aunque en general es de la siguiente forma:

Ping [-opcion] host [tamaño] [paquetes]

- Opción: activa diversas opciones del ping.
- Host: Es el destino representado con un nombre simbólico o una dirección IP.
- Tamaño: el tamaño del paquete.
- Paquete: Él número de paquetes a enviar.

Ping es útil para verificar instalaciones de TCP/IP.

- **Traceroute o tracert**

El programa traceroute permite determinar la ruta que siguen los datagramas IP de host a host. Se basa en el protocolo ICMP para enviar un datagrama IP, si el datagrama tiene un tiempo de vida (TTL) de 1 al host destino. El primer router que vea al datagrama decrementara el TTL a 0 y devolverá el mensaje ICMP tiempo excedido, además de eliminar el datagrama, de esta forma se identifica el primer router del camino. Este proceso se puede repetir sucesivamente con TTLs mayores para identificar la serie de routers que se encuentran en el camino hasta el host de destino. El traceroute lo que hace es enviar al host de destino datagramas UDP que hacen referencia a un numero de puerto fuera del rango usado normalmente, el traceroute determinara cuando se alcanzo el host de destino al recibir el mensaje ICMP puerto inalcanzable.

- **Finger**

La utilería finge recupera información desde un host remoto. Muestra información de que usuarios están conectados al host remoto. Si no se especifica ningún usuario, la información será típicamente una lista de todos los usuarios conectados actualmente al host.

- **NSLOOKUP**

NSLOOKUP examina las bases de datos del DNS. Se utiliza para regresar la dirección IP de algún dominio cualquiera.

- **NBTSTAT**

NBTSTAT. Registra el NetBIOS.

- **NETSTAT**

NETSTAT se usa par consultar a TCP/IP acerca del estado de la red en la que se halla el host local. Se trata de una herramienta útil para la depuración. Proporciona información sobre:

- Las conexiones TCP activas en el host local.
- El estado de todos los servidores TCP/IP del servidor local y de los sockets que usan.
- Dispositivos y enlaces usados por TCP/IP.

- Las tablas de encaminamiento IP usadas en el host local.

❖ Protocolos para aplicaciones de ejecución remota.

- **Telnet**

Telnet es un protocolo que permite emular terminales. Proporciona una interfaz estandarizada a través de la cual un programa de un host (el cliente de Telnet) puede acceder a los recursos de otros hosts (servidores de Telnet) a través de la red como si el cliente fuera una terminal local conectada al servidor. Telnet se puede usar tanto en LANs como en WANs. El telnet moderno es un emulador de terminal versátil debido a las muchas opciones que han evolucionado desde hace 20 años, estas opciones le dan la capacidad de transferir datos binarios, soportar macros de bytes, emular terminales graficas y transportar información para soportar administración terminal centralizada. Proporciona el servicio NFS (Network File Systems), NFS es un conjunto de protocolos desarrollados por Sun Microsystems para permitir a múltiples maquinas tener acceso a las direcciones de cada una de las otras de manera transparente. Las terminales heterogéneas se conectan usando un protocolo de terminal virtual (VTP) que realiza las siguientes funciones:

- Establecimiento y mantenimiento de conexiones
- Control del dialogo para negociar las acciones permitidas durante la conexión.
- Creación y mantenimiento de una estructura que representa el estado del terminal.
- Traslación de las características del terminal real a la representación normalizada.

El objetivo de VTP es transformar las características de un terminal real en un terminal normalizado. Debido a la gran diversidad normalmente solo se definen las funciones básicas.

EL VTP tiene las ejecuta las siguientes fases de operación:

- Establecimiento y liberación de la conexión.
- Negociación para determinar el conjunto del dialogo entre los extremos de la conexión.
- Control del intercambio de información y de mandatos.

Telnet se basa en tres principios:

- El concepto de terminal virtual de red NVT (Network Virtual Terminal): Una NVT es un dispositivo imaginario que posee una estructura básica común a una amplia gama de terminales reales. Cada host mapea las características de su propia terminal sobre las de su correspondiente NVT.
- Simetría entre terminales y procesos.
- Opciones negociadas: Se pueden negociar diversas opciones ya que muchos hosts pueden desear suministrar servicios adicionales mas allá de los disponibles en NVT.

Cuando un usuario invoca la aplicación Telnet un proceso de usuario se convierte en la aplicación cliente. Este cliente establece una conexión virtual mediante TCP con el servidor a través de la cual se comunican ambas entidades, los dos hosts comienzan verificando que existe una comprensión mutua entre ellos. Después de conectarse el servidor Telnet y el cliente entran en una fase de negociación que determina las opciones que cada lado puede soportar para la conexión, cada extremo de la conexión intenta implementar todas las opciones que maximizan el desempeño de los sistemas involucrados, ya establecida la conexión el cliente acepta los datos que teclea el usuario y los envía al servidor.

❖ Protocolos para transferencia de archivos

La copia de ficheros de una maquina a otra es una de las operaciones más frecuentes realizada por medio de las redes, esta transferencia de datos entre un cliente y un servidor puede producirse en cualquier dirección.

El acceso a archivos compartidos puede hacerse en línea o mediante copia completa. El acceso en línea permite que múltiples programas accesen a un archivo concurrentemente y que los cambios realizados en el archivo se apliquen inmediatamente y estén disponibles para todos los procesos que acceden al archivo. El acceso por copia permite que un programa realice una copia del archivo a su almacenamiento local, realice los cambios pertinentes y que transfiera la versión modificada al sitio original. La transferencia de archivos funciona en dos pasos, primeramente se obtiene una copia del archivo, por lo que el usuario invoca a un programa cliente para que transfiera el archivo especificándole el computador remoto donde se localiza el archivo y realizando una autorización de la operación. El cliente contacta con el servidor remoto y pide una copia del archivo, una vez realizada la transferencia el usuario finaliza el cliente y el programa accede a ese archivo en su sistema local para leer y actualizar. El cliente y el servidor deben estar de acuerdo en autorizaciones, propiedades de archivos, protecciones y formato de datos.

- **Protocolo FTP**

El protocolo de transferencia de archivos FTP (File Transfer Protocol) es el protocolo usado para la transferencia de archivos. Proporciona elementos básicos de compartición de archivos entre hosts, el servicio XDR (Exchange Data Represent). FTP hace uso de TCP para crear conexiones fiables entre los extremos. Se establecen dos conexiones, Fig. 3.1.1.20, la primera es para el login la cual mediante el protocolo Telnet se crea una conexión virtual para la información de control y la segunda crea una conexión TCP separada para transferir datos.

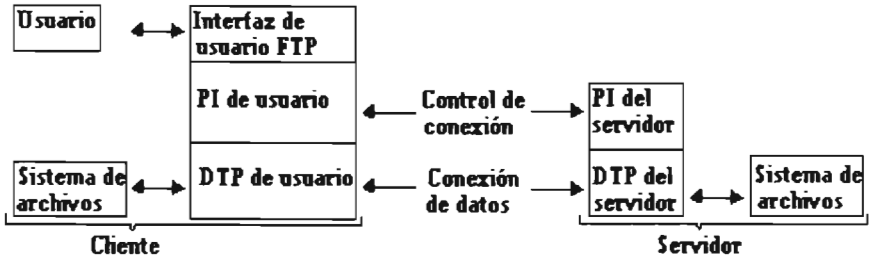


Fig. 3.1.1.20 Principios de FTP

La información de control usa una imagen del protocolo Telnet para intercambiar comandos y mensajes entre hosts. Las tramas de control FTP son intercambios Telnet y pueden contener comandos Telnet y negociación de opciones, sin embargo la mayoría de las tramas de control son texto ASCII simple y pueden ser clasificadas como comandos FTP o mensajes FTP. Para realizar las transferencias proporciona las siguientes facilidades:

- Acceso interactivo. Aunque fue diseñado para usarse por programas, su implementación proporciona al usuario una interfaz con servidores remotos para importar o exportar archivos.

- Especificaciones de formato. Permite al cliente especificar el tipo y formato de los datos por ejemplo ASCII o binarios.
- Control de autenticación. FTP le exige al cliente que se identifique mediante su nombre de usuario y su contraseña.

Las implementaciones FTP permiten el acceso concurrente de varios clientes que emplean TCP para conectarse al servidor. En el servidor el proceso maestro acepta y lleva a cabo las peticiones de conexión del cliente pero otro proceso maneja la transferencia de datos.
En el funcionamiento de FTP el proceso cliente se conecta al servidor mediante un login para lo cual necesitar un nombre de usuario y password para acceder a ficheros y directorios, el usuario que inicia la conexión asume la función de cliente, mientras que el host remoto adopta la función de servidor.
Se establece una nueva conexión para cada archivo que se vaya a transmitir. La conexión para transferencia de datos y los procesos para transferencia de datos se crean dinámicamente según se van necesitando, la conexión de control permanece activa mientras dure la sesión FTP. Cuando la conexión de control desaparece la sesión finaliza y los procesos de ambos extremos finalizan la transferencia de datos. Para la asignación de los puertos de FTP, cuando el cliente se conecta al servidor emplea un puerto aleatorio y en el servidor se usa el puerto 21 para la transferencia de los datos, el cliente no puede usar los mismos puertos usados en la conexión de control por lo que obtiene un puerto no usado de su maquina y trasfiere los datos al puerto 20 del servidor. Algunas operaciones que se pueden realizar con FTP son:
- Conexión a un host remoto.
- Selección de un directorio.
- Listado de ficheros disponibles para una transferencia.
- Especificación del modo de transferencia.
- Copiar fichero de/o al host remoto.
- Desconectar del host remoto.

Para gestionar todas estas operaciones mediante el dialogo Telnet el cliente manda comandos y el servidor contesta con códigos de respuesta, estas respuestas incluyen comentarios para el usuario, pero el cliente usa solo los códigos, los códigos tiene tres dígitos siendo el primero el mas significativo, estos códigos se muestran en la tabla 3.1.1.3

Código de respuesta	Descripción
1xx	Respuesta preeliminar positiva
2xx	Respuesta de completamiento positiva
3xx	Respuesta intermedia positiva
4xx	Respuesta de completamiento negativa transitoria
5xx	Respuesta de completamiento negativa permanente

Tabla 3.1.1.3 Códigos de respuesta de FTP

- **Protocolo TFTP Trivial FTP.**

TFTP Es un protocolo sencillo (de ahí su nombre trivial FTP) para aplicaciones que no requieren mucha interacción entre cliente y servidor. Se aplica a operaciones de transferencia de archivos donde no es necesaria una autenticación ya que no soporta servicios de directorio de autentificación de usuarios. Tiene asignado el puerto 69 y utiliza el protocolo de transporte UDP. Soporta escritura y lectura de archivos. La corrección de

errores la ejecuta mediante un mecanismo de parada y espera para controlar el flujo de información. Es un protocolo inseguro.
Cualquier transferencia comienza con una solicitud para leer o escribir un fichero. Si el servidor concede la solicitud, se abre la conexión y el fichero se envía en bloques consecutivos de 512 bytes (longitud fija). Cuando se envía el primer paquete se establece una interacción entre el cliente y servidor. Los bloques del fichero se numeran correlativamente comenzando con 1. Cada paquete de datos debe ser reconocido mediante un paquete de reconocimiento antes de que se envíe el siguiente paquete. La cabecera de los datos especifica el bloque que contiene y por cada confirmación contiene el número de bloque que confirma su recepción. Se asume el final del archivo cuando se recibe un paquete de menos de 512 bytes. Cada extremo implicado implementa un temporizador y una retransmisión. Si vence el temporizador del emisor, este retransmite el ultimo bloque de datos. Si vence el temporizador del receptor este retransmite la ultima confirmación. La mayoría de los errores provocaran la terminación de la conexión (falta de confiabilidad). Si un paquete se pierde en la red se producirá un timeout, tras el que se efectuara la retransmisión del ultimo paquete (de datos o de reconocimiento). Los paquetes usados en las transferencias con TFTP se muestran en la Fig. 3.1.1.21.

Paquete RRQ/WRQ

2 bytes	string	1 byte	string	1 byte
Código de operación	Nombre del archivo	0	Modo	0

Paquete de Datos

2 bytes	2 bytes	Hasta 512 bytes de datos
Código de operación	# de bloque	Datos

Paquete ACK

2 bytes	2 bytes
Código de operación	# de bloque

Paquete de error

2 bytes	2 bytes	string	1 byte
Código de operación	# de bloque	Mensaje de error	0

Fig. 3.1.1.21 Paquetes TFTP

Los 5 paquetes de TFTP son:

Código de operación	Operación
1	Read Request RRQ (Solicitud de lectura)
2	Write Request WRQ (Solicitud de escritura)
3	Data (Datos)
4	Acknowledgment ACK (Reconocimiento)
5	Error

TFTP comúnmente es muy usado para bajar y subir configuraciones de equipos por medio de la red y en otras ocasiones para arrancar computadoras desde un servidor.

- **Impresión**
  - LPR Line Printer remote. Impresión remota. Permite gestionar una o varias impresoras, con uno o varios usuarios que envían distintos tipos de documentos. Para ello en el sistema debe estar corriendo un programa de impresión en línea LPD (Line Printer Daemon), cuyas impresiones pueden ser encoladas en una cola de impresión LPQ (Line Printer Queue).

- **Protocolo SMTP**

El correo electrónico es un servicio muy popular debido a que realiza la transferencia de información de manera rápida y eficiente, el correo electrónico (e-mail) es una de las aplicación TCP/IP mas usada. Los protocolos de correo básicos proporcionan intercambio de correo y mensajes entre hosts TCP/IP. Existen dos partes en un sistema de correo, el proceso front end que acepta el correo del usuario, lo coloca en una área de spool, otro proceso extrae esos mensajes del área de spool y lo envía al destino. Los mensajes recibidos se depositan en buzones hasta que el destinatario los recibe.

El protocolo simple de transferencia de correo electrónico SMTP (Simple Mail Transfer Protocol) es un estándar para el intercambio de correo entre dos maquinas, es un servicio de correo modelado en el servicio FTP, transfiere los mensajes de correo entre sistemas y proporciona notificación con respecto al correo de entrada. Especifica el formato de los mensajes y que mensajes se deben intercambiar, no especifica como se debe almacenar el correo o la frecuencia de envío de mensajes. El protocolo trabaja en colaboración con un programa de correo de usuario (por ejemplo Outlook Express) que se encarga de transferir de un sistema a otro el correo generado por los usuarios con sus programas de correo.

SMTP es un protocolo cliente/servidor, el cliente SMTP es el que inicia la sesión (el emisor) y el servidor el que responde a la solicitud de sesión (el receptor). Como el cliente suele actuar como servidor para un programa de correo del usuario, es más sencillo referirse a el cómo emisor SMTP y al servidor como receptor SMTP.

SMTP define los mensajes de control que usan los sistemas en el intercambio de mensajes de correo electrónico:

- Como resultado de la solicitud de correo del usuario, el emisor SMTP establece un canal de transmisión bilateral con el receptor SMTP.
- Verifica que la conexión se encuentra establecida correctamente.
- Los comandos SMTP son generados por el emisor SMTP y enviados al emisor SMTP.
- Identifica al remitente.
- Las respuestas a los comandos SMTP son enviadas del emisor SMTP al receptor SMTP.
- Acuerda los parámetros de transmisión.
- Transmite el mensaje.

La transferencia de correo se realiza de la siguiente forma:

- Una vez que el canal es establecido el emisor SMTP envía un comando MAIL, indicando el emisor de correo.
- Si el receptor SMTP puede aceptar el correo, devuelve una respuesta OK.
- El emisor SMTP entonces envía un comando RCPT identificando un recipiente de correo.

- Si el receptor SMTP puede aceptar correo para ese recipiente, devuelve una respuesta OK, si no, rechaza la solicitud (pero no la transacción completa de correo).
- El emisor SMTP y el receptor SMTP pueden negociar varios recipientes.
- Cuando los recipientes han sido negociados el emisor SMTP envía los datos del correo.
- Si el receptor SMTP procesa exitosamente los datos del correo devuelve una respuesta OK.
- El dialogo es cerrado.

SMTP se basa en la entrega punto a punto, un cliente SMTP contactara con el servidor SMTP del host destino directamente para entregar el correo. Guardara el correo hasta que se haya copiado con éxito en el receptor.

Cada mensaje SMTP tiene:

- Una cabecera o sobre: especifica la información para que el mensaje pueda ser enviado y recibido por el destinatario. La cabecera termina con una línea nula.
- Contenido: Todo lo que hay detrás de la línea nula es el cuerpo de mensaje, este cuerpo es la información dirigida al destinatario que puede ser texto, imagenes o multimedia.

El mensaje consta de sobre y contenido. El contenido es la información dirigida al destinatario que puede ser, texto, imágenes o multimedia. El flujo de datos de SMTP se observa en la fig. 3.1.1.22.

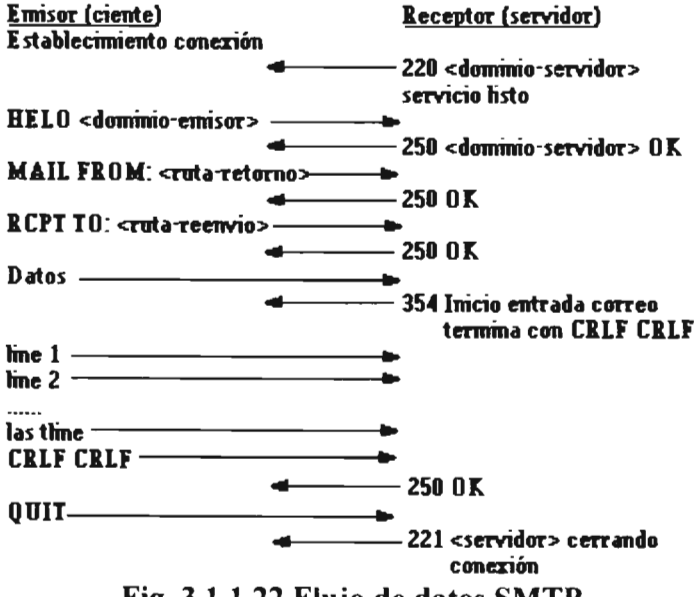


Fig. 3.1.1.22 Flujo de datos SMTP

1. El emisor SMTP establece la conexión TCP con el SMTP destino y espera el mensaje 220 Servicio listo.
2. Se envía un HELO con el que el receptor se identifica devolviendo su dominio, el emisor usa este mensaje para verificar que se contacto con el SMTP destino.
3. El emisor inicia la transacción enviando el comando MAIL al servidor, el cual contiene la ruta de regreso al emisor para informar de errores. La ruta además del par

buzon@nombre de dominio contienen una lista de los hosts de encaminamiento. El receptor responde con un 250 OK.
4. En el segundo paso de intercambio de correo le da al servidor SMTP el destino del mensaje con comandos RCPT TO que son respondidos con 250 OK.
5. El emsior envía el comando DATA para notificar que a continuación se envían los contenidos del mensaje, el servidor responde con un 354.
6. El cliente envía los datos línea a línea hasta terminar con CRLF CRLF y el reconocimiento 250 OK del servidor.
7. Por ultimo si ya no se tienen mas mensajes que enviar se cierra la conexión, o se pone el emisor en modo de recibir mensaje con el comando TURN el cual invierte los papeles de emisor y receptor o el emisor tiene otro mensaje que enviar y vuelve al paso 3.

Existen otros protocolos con funciones adicionales en el correo electrónico como son:
- MIME (Multipurpose Internet Mail Extensions) y su versión segura S-MIME para transmisión de mensajes multimedia.
- IMAP (Internet Messaging Access Protocol) que aporta funciones de almacenamiento y envío, permiten que los usuarios accesen a su correo desde diversos terminales, desde su oficina y desde su domicilio con RTB.

- **Protocolo POP3**

El protocolo POP3 (Post Office Protocol) es un cliente que proporciona el acceso a los mensajes de los servidores SMTP, esta diseñado para permitir a las estaciones de trabajo dinámicamente accesar a un recipiente de mensajes en un host servidor de forma eficaz. Se usa para permitir a la estación que recupere el correo que el servidor esta guardando para el. El servidor de POP3 inicia el servicio monitoreando el puerto TCP 110. Cuando un cliente desea hacer uso del servicio establece una conexión con el servidor. Cuando la conexión es establecida el servidor POP3 envía una confirmación. El cliente y el servidor POP3 entonces intercambian comandos y respuestas hasta que la conexión es cerrada o abortada. Las transmisiones POP3 parecen como mensajes de datos entre estaciones, los mensajes son ya sea comandos o mensajes de respuesta. Una sesión POP3 involucra esta serie de pasos:

- Una vez que la conexión TCP ha sido abierta, el servidor de POP3 envía el mensaje de bienvenida.
- La sesión entra en un estado de autorización, el cliente debe identificarse ante el servidor.
- El servidor reserva los recursos asociados con el recipiente del cliente. El cliente solicita acciones en el servidor POP3.
- Cuando el cliente ha generado el comando QUIT la sesión entra en un estado de actualización. El servidor desocupa los recursos involucrados y concluye la sesión.
- Cierra la conexión TCP.

- **Protocolo IMAP4**

El protocolo de acceso de mensajes de Internet IMAP (Internet Message Access Protocol) permite a un cliente acceder y manipular mensajes de correo electrónico sobre un servidor. Permite la manipulación de carpetas de mensaje remoto llamadas mailboxes de forma que es funcionalmente equivalente a los mailboxes locales, proporciona la capacidad para que un cliente fuera de línea se pueda resincronizar con el servidor. Incluye operaciones de

creación, borrado y renombrado de mailboxes, chequeo de nuevos mensajes, remover mensajes permanentemente, configurar y borrar banderas, búsqueda y selección de atributos de mensajes, textos y porciones. Los mensajes son accesados por el uso de números. Estos números son, ya sea mensajes de números de secuencia o identificadores únicos. IMAP4 consiste de una secuencia de mensajes textuales que contienen comandos, mensajes de estado, etc.

- **Protocolo BOOTP**

Las redes de área local hacen posible usar hosts sin disco como estaciones de trabajo, routers, concentradores de terminales, etc. Los hosts sin disco requieren de algun mecansimo para el arranque remoto sobre una red. El protocolo BOOTP (Bootstrap Protocol) se usa para realizar arranques remotos sobre redes IP, permite que una pila de IP mínima sin información de configuración almacenada en la ROM obtenga información suficiente para comenzar el proceso de descargar el código de arranque necesario. El protocolo en si, no define como se realiza esta descarga pero habitualmente se emplea TFTP.

También se puede hacer uso de este protocolo para la asignación de direcciones IP en lugar del protocolo ARP, una maquina que se pone en funcionamiento por primera vez puede usar el protocolo BOOTP para obtener la dirección IP e información sobre su sector de arranque. El proceso es el siguiente.

1. El cliente determina su propia dirección MAC (dirección de hardware). la cual normalmente se almacena en una ROM del hardware.
2. El cliente BOOTP envía su dirección MAC en un datagrama UDP al servidor. Si el cliente conoce su dirección IP y/o la del servidor debería usarlas, pero en general los clientes BOOTP carecen de configuración IP en absoluto. Si el cliente desconoce su dirección IP emplea la 0.0.0.0. Si desconoce la dirección IP del servidor utiliza la dirección de broadcast limitado (255.255.255.255). Su puerto asignado es el 67 y usa el protocolo UDP.
3. El servidor cuando recibe el datagrama busca la dirección MAC del cliente en su configuración que contiene la dirección IP del cliente. El servidor rellena los campos restantes del datagrama UDP y lo devuelve al cliente por el puerto 68. Esto lo puede hacer de tres formas:
   - Si el cliente conoce su propia dirección IP incluida en el datagrama BOOTP. el servidor devuelve directamente el datagrama a esa dirección. Es probable que la cache ARP en la pila de protocolos del servidor desconozca la dirección hardware que corresponde a la dirección IP, por lo que hará uso de ARP para determinarla.
   - Si el cliente desconoce su propia dirección IP (0.0.0.0), el servidor la averigua con su propia cache de ARP. Aquí hay dos soluciones posibles:

   a) Si el servidor tiene algún mecanismo para actualizar directamente su cache sin usar ARP lo utiliza y envía directamente el datagrama
   b) Si el servidor no puede utilizar su propia cache debe enviar una respuesta en forma de broadcast
4. Cuando el cliente BOOTP recibe la respuesta. graba su dirección IP con lo que ya puede responder a peticiones ARP. Una vez que ha procesado la respuesta puede proceder con la transferencia del fichero de arranque y ejecutar el proceso de arranque completo. El proceso de arranque completo reemplaza la pila mínima de

IP usada por BOOTP y TFTP por una pila IP normal transferida como parte del fichero de arranque que contiene la configuración correcta para el cliente.

Los campos del mensaje que usa el protocolo BOOTP se muestran en la Fig. 3.1.1.23:

8 bits	8 bits	8 bits	8 bits
Tipo	Tipo de encabezado	Longitud de encabezado	Cuenta de saltos
Identificador de transacción			
Segundos		Cero	
Dirección IP del cliente			
Dirección Ip de respuesta			
Dirección IP del servidor			
Dirección IP del gateway			
Dirección del hardware del cliente (16octetos)			
Nombre de host del servidor (64octetos)			
Nombre de archivo de arranque (64octetos)			
Area del vendedor (64 octetos)			

Fig. 3.1.1.23 Formato del mensaje BOOTP

- Tipo: Indica si el mensaje es una solicitud (1) o una respuesta (0).
- Cabecera: Identifica el tipo de dirección de hardware, por ejemplo ethernet (1), IEEE802 (6).
- Longitud-H: Identifica la longitud de la dirección de hardware en octetos. Las de ethernet son de 6 bytes.
- Contador de saltos: Se usa cuando BOOTP pasa a través de varios gateways. El cliente lo pone a 0. Cada paso por un gateway aumenta en 1 el contador con el fin de detectar bucles. Se sugiere que un valor de 3 ya es un bucle.
- Identificador de transacción: Es un numero aleatorio usado para comparar la solicitud con la respuesta que genera.
- Segundos: Calcula el tiempo transcurrido desde el envío de la solicitud hasta la recepción de la respuesta.
- Cero. El bit más significativo de este campo se usa como bandera de broadcast, todos los demás bits deben estar a cero ya que están reservados para uso futuro. Los servidores BOOTP tratan de entregar los mensajes de respuesta directamente al cliente usando unicast, para ello la dirección IP en la cabecera se pone al valor de la dirección IP fijada por el servidor y la dirección MAC a la dirección hardware del cliente BOOTP, si un host no puede recibir un datagrama IP en unicast hasta saber su dirección IP, el bit de broadcast se pone a 1 para indicar al servidor que el mensaje de respuesta se debe enviar como un broadcast en IP y MAC.
- Dirección IP del cliente: Si se conoce se pone la dirección, si no se pone a cero.
- Dirección IP de respuesta. Fijada por el servidor si el valor del campo anterior es 0.0.0.0.
- Dirección IP del servidor: Si se conoce se pone la dirección del servidor, si no se pone la de broadcast.
- Dirección IP del gateway: Se pone la dirección del gateway, si no existe un gateway se pone a cero.
- Dirección del hardware del cliente: Lo completa el cliente y la usa el servidor para identificar cual de los clientes registrados esta arrancando.
- Nombre del servidor host: Campo opcional, puede estar en cero.

- Nombre de archivo de arranque: El cliente deja este campo vacío o especifica un nombre genérico indicando el tipo de archivo de arranque a usar. El servidor devuelve el nombre completo del fichero o bien el de un fichero de arranque adecuado para el cliente.
- Area del vendedor: Area del distribuidor opcional, se recomienda que el cliente llene los 4 primeros bytes con magic cookie, si no se usa el cliente debería utilizar 99.130.83.99 seguido de una marca de fin y fijar los bits restantes a cero.

El esquema de funcionamiento de BOOTP tiene una restricción por el uso del broadcast limitado por lo que el servidor debe estar en la misma subred que el cliente. La retransmisión BOOTP es un mecanismo para que los routers trasmitan solicitudes BOOTP.

- **Protocolo DHCP**

El protocolo de asignación dinámica de host DHCP (Dynamic Host Configuration Protocol) pasa información de configuración a los hosts en una red TCP/IP. Se basa en el protocolo BOOTP añadiendo la capacidad de asignar automáticamente direcciones de red utilizables y opciones de configuración adicionales. Consiste en dos componentes: un protocolo para entrega de parámetros de configuración desde un servidor DHCP a un host y un mecanismo para asignaciones de direcciones de red IP a los clientes que lo soliciten.
DHCP soporta tres mecanismos para la asignación de direcciones IP:
1. Asignación automática. En este modo el protocolo asigna al host una dirección IP permanente.
2. Asignación dinámica. El DHCP asigna una dirección IP por un periodo de tiempo limitado, como un arrendamiento. Este es el único mecanismo que permite la reutilización automática de direcciones que ya no son necesitadas por los hosts a los que estaban asignadas
3. Asignación manual. La dirección del host es asignada por el administrador de red.
El procedimiento del cliente para obtener su dirección es el siguiente:

1. Envía un mensaje al servidor DHCP solicitando una dirección IP.
2. El servidor responde ofreciendo varias direcciones que tiene disponibles.
3. El cliente selecciona una y envía una solicitud de uso de la dirección al servidor DHCP.
4. El servidor DHCP admite la solicitud.

Estas direcciones se conceden por un tiempo determinado, finalizado ese tiempo el cliente debe solicitar la renovación de la concesión o esta se pone como disponible, si la renovación no se puede efectuar se reasigna otra. El formato del encabezado es mostrado en la Fig. 3.1.1.24.

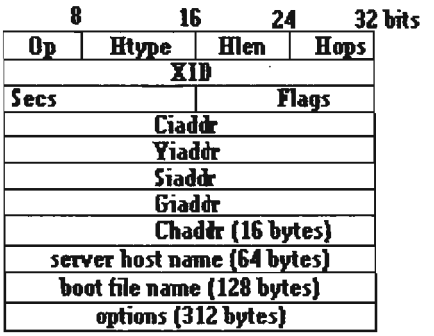


Fig. 3.1.1.24 Estructura del encabezado DHCP

- Op: El código del mensaje de operación. Los mensajes pueden ser BOOTREQUEST (1) o BOOTREPLY (2).
- Htype: Tipo de dirección de hardware como ethernet (1), IEEE 802 (6).
- Hlen: Longitud en bytes de la dirección de hardware, ethernet son 6 bytes.
- Hops: El cliente lo pone a 0. Cada router que transmite la solicitud a otro servidor lo incrementa con el fin de detectar bucles, un valor de 3 indica un bucle.
- XID: Identificador de la transacción. Numero aleatorio usado para comparar la solicitud con la respuesta que genera. Si un host no puede recibir un datagrama IP en unicast hasta saber su propia dirección IP, el broadcast se debe poner a 1 para indicar al servidor que el mensaje se debe enviar como un broadcast en IP y en MAC, de otra forma se pone a 0.
- Secs: Los segundos transcurridos desde que el cliente comenzó la adquisición de dirección, proceso de renovación o proceso de arranque.
- Flags: Las banderas. Los bits más significativos de este campo se usa como bandera de broadcast. Todos los demás bits deben ser 0. Los servidores DHCP tratan de entregar los mensajes al cliente usando unicast. La dirección de destino en la cabecera IP se pone al valor de la dirección IP fijada por el servidor DHCP y la dirección MAC a la dirección hardware del cliente DHCP.
- Ciaddr: Dirección IP fijada por el cliente, o bien su dirección IP real, o 0.0.0.0.
- Yiaddr: La dirección IP del cliente fijada por el servidor si el valor del campo anterior es 0.0.0.0.
- Siaddr: La dirección IP del siguiente servidor para usar en el arranque.
- Giaddr: La dirección IP del agente retransmisor usada en el arranque si se usa retransmisión BOOTP.
- Chaddr: La dirección hardware del cliente y usada por el servidor para identificar cual de los clientes registrados esta arrancando.
- Server host name: Nombre opcional del host servidor acabado en X'00'.
- Boot file name: El cliente puede dejar este campo vacío o especificar un nombre genérico indicando el tipo de fichero de arranque a usar.
- Options: Los primeros 4 bytes del campo de opciones del mensaje DHCP contienen el cookie (99.130.83.99).

El protocolo DHCP permite un almacenamiento persistente de los parámetros de red de los clientes, para ello almacena una entrada con un valor y una clave para cada cliente, el valor contiene los parámetros de configuración del cliente.

Un host debería usar DHCP para readquirir o verificar su dirección IP y sus parámetros de configuración siempre que cambien los parámetros de su red local.

- **Protocolo HTTP**

La WWW (World Wide Web) se convirtió en el servicio con más potencial en todos los sectores de la sociedad. Los documentos de WWW pueden contener tanto texto, como gráficos, sonidos e imágenes dinámicas que están enlazadas mediante hipertexto. Las paginas con hipertexto son creadas con el lenguaje HTML (Hipertext Markup Language), XML (Extended Markup Language) o el WML (Wireles Markup Language) para aplicaciones inalámbricas. Las características del hipertexto son que los documentos contienen hipervínculos o palabras que hacen referencia a otros documentos relacionados al tema. En el texto las palabras o frases se realzan y al seleccionarlas pasan a la siguiente página del mismo documento o se conectan a otra pagina en el ciberespacio en cualquier parte del mundo. Para navegar a través de este tipo de documentos o paginas Web se usan los visualizadores como Mosaic, Netscape, o Explorer. Para identificar las paginas WEB dentro dela telaraña se utilizan los localizadores uniformes de recursos URL (Uniform Resource Locator) que están asociados unívocamente a cada pagina, los URLs indican como se llama la pagina, su localización y como se accede a ella, se compone de tres partes: un nombre que representa de forma única la pagina, el nombre DNS del servidor en el que se encuentra la pagina y el protocolo, el protocolo normalmente es http, aunque se pueden usar otros como ftp o telnet dependiendo si se quiere visualizar paginas por medio del navegador o transferir archivos, etc.

Cuando se localiza una página se producen los siguientes procesos:

- El visualizador identifica el URL.
- Solicita al DNS la dirección IP.
- El visualizador solicita una conexión TCP con el puerto 80 (protocolo http) de la dirección IP recibida.
- El visualizador emite un comando GET para bajar la pagina.
- El servidor envía el archivo correspondiente al cliente local.

El protocolo de transferencia de hipertexto http (Hyperterminal Transfer Protocol) es un protocolo a nivel aplicación con la ligereza y velocidad necesarias para sistemas de información hipermedia distribuidos y colaborativos. El protocolo establece comunicación entre el cliente browser y el servidor Web, sigue el esquema cliente /servidor, y realiza conexiones con el protocolo TCP, es usado para transportar lenguajes HTML de la web, cada vez que se realiza una transacción se establece una nueva conexión. Los mensajes de este protocolo son pasados en un formato similar al que usa el correo de Internet y MIME. http se basa en el esquema solicitud contestación. Un cliente establece una conexión con el servidor y envía una solicitud al servidor en la forma de un método de solicitud URI (Uniform Resource Identifier) y la versión del protocolo seguido por un mensaje del tipo MIME con los parámetros de la solicitud, la información de cliente y posiblemente el cuerpo del mensaje. El servidor responde con un status line incluyendo la versión del protocolo del mensaje y un código de éxito o fracaso, seguido por un mensaje del tipo MIME con información del servidor y posiblemente el cuerpo del mensaje. Este protocolo divide los mensajes en uno o más paquetes para ser enviados individualmente a través de Internet. Transmite los datos en octetos de 8 bits. Como transmite documentos de texto y archivos binarios, utiliza un subconjunto de las especificaciones MIME para encapsular y codificar los archivos a ser transmitidos. Cada mensaje http se compone de un encabezado

y un cuerpo. El encabezado provee información acerca del mensaje, tipo de mensaje, identificación y capacidades del host, información administrativa y la descripción del cuerpo. El cuerpo de mensaje contiene un bloque de información que representa un archivo enviado o una forma de datos HTML. El formato del paquete de petición se observa en la Fig. 3.1.1.25

Fig. 3.1.1.25 Estructura del paquete e petición

- Method: El método a ser ejecutado sobre el recurso.
- Request URI: El Uniform Resource Identifier (URI), el recurso sobre el cual se aplica la petición, por ejemplo un recurso de red.
- http versión: La versión http que es usada.

El formato del paquete de respuesta es el de la Fig. 3.1.1.26

Fig. 3.1.1.26 Estructura del paquete de respuesta

- http versión: La versión de http que es usada.
- Status code: Un código entero de 3 dígitos resultado del intento de entender y satisfacer la petición.
- Reason-phrase: Una descripción textual de status code.

- **SHTTP**

El protocolo http seguro (Secure http) proporciona mecanismos de comunicación segura entre un par cliente/servidor http para permitir transacciones comerciales espontáneas para un amplio rango de aplicaciones. Es un protocolo flexible que soporta múltiples modos de operación ortogonales, mecanismos de administración clave, modelos confiables, algoritmos criptográficos y formatos de encapsulación a través de la opción de negociación entre parejas para cada transacción. Sintacticamente los mensajes de SHTTP son parecidos a los de http, componiéndose de una petición o línea de estado, seguida por encabezados y un cuerpo, aunque el rango de encabezados es diferente y los cuerpos están criptográficamente mejorados.

- **DNS**

Todo host IP tiene una dirección IP y un nombre de equipo, por lo cual se puede iniciar una conexión indicado la dirección IP del host o el nombre del equipo, la segunda opción es preferible ya que es más fácil recordar el nombre que la dirección IP. Para esto se puede implementar un servidor DNS, un archivo LMHOSTS, servidor WINS o la resolución de NETBIOS sobre nodos TCP/IP.

Inicialmente esto se podía hacer con el archivo local Hosts donde se definían en dos listas de columna la dirección IP seguida del nombre completo de la maquina, el archivo se situaba en el mismo lugar de TCP/IP determinado por el sistema operativo del equipo. El archivo local LMHOSTS es igual que el hosts pero además puede usar palabras clave en su definición. Asimismo el mapeado de nombres a direcciones se mantenía en el fichero HOSTS.TXT mantenido por el NIC y al que accesaban u obtenían los hosts vía FTP, este era conocido como espacio de nombres plano.

El sistema de nombres de dominio DNS (Domain Name System) es un conjunto de protocolos y servicios sobre una red TCP/IP que permite los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos en vez de memorizar y usar sus direcciones IP. De esta forma el DNS permite que un programa ejecutándose en un host le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

El proceso de mapear nombres a direcciones se conoce como resolución de nombres de dominio y lo proporcionan sistemas independientes cooperativos, llamados servidores de nombres. Un servidor de nombres es un programa servidor que responde a peticiones de un cliente llamado procesador de nombres. Cada procesador de nombres esta configurado con el nombre de servidor que va a usar (y una lista de servidores alternativos con los que contactara sí el servidor primario no esta disponible). El usuario proporciona el nombre de un host y el programa de usuario emplea una rutina de librería llamada stub para comunicarse con un servidor de nombres que resuelve el nombre del host en una dirección IP y se la devuelve al stub que a su vez lo devuelve al programa principal. El servidor de nombres puede obtener la respuesta de su cache de nombres, su propia base de datos o cualquier otro servidor de nombres.

El sistema usa servidores distribuidos a lo largo de la red para resolver el nombre de un host IP en una dirección IP. Posteriormente con el DNS se usa una base de datos para resolver el nombre del computador.

Por la forma de distribuir los servidores se usa el concepto de espacio de nombres distribuido. Los nombres simbólicos se agrupan en zonas de autoridad o zonas. En cada zona uno o más hosts mantiene una base de datos de nombres simbólicos y direcciones IP y proporciona la función de servidor para los clientes que deseen traducir nombres simbolicos a direcciones IP. Estos servidores de nombres locales se interconectan lógicamente en un árbol jerárquico de dominios. Los nombres de cada zona se administran con independencia de los de otras zonas. La autoridad sobre zonas se delega en los servidores de nombres. La división por zonas se realiza utilizando registros de recursos guardados en el DNS. El comienzo de un dominio esta mas cerca de la raíz del árbol que a sus terminaciones. En la raiz no puede haber servidores de nombres superiores para delegar autoridad, la autoridad para la raíz se delega en un conjunto de servidores de nombres de raíz. El resultado de este esquema es:

- En vez de tener un servidor central para la base de datos, el trabajo implicado en mantenerla se reparte entre los hosts a lo largo y ancho del espacio de nombres.
- La autoridad para crear y cambiar nombres simbólicos de hosts y la responsabilidad de mantener una base de datos para ellos le corresponde a la organización propietaria de la zona que los contiene.
- Para el usuario hay una sola base de datos que trata la resolución de direcciones.

Resolución de dominios

La resolución de dominios se realiza en un esquema cliente/servidor. La función del cliente (resolver o name resolver) es transparente al usuario y es invocada por una aplicación para mapear nombres de alto nivel a direcciones IP o viceversa. El servidor de nombres (servidor de nombres de dominio) es una aplicación servidora que traduce los nombres de alto nivel de las maquinas a direcciones IP. El proceso se puede hacer de dos maneras:

1.Con un programa llamado full resolver distinto del programa de usuario que envía todas las peticiones al servidor de nombres. El servidor de nombres almacena las respuestas para su uso futuro.

2. Con una rutina stub resolver enlazada con el programa de usuario que envía las peticiones a un servidor de nombres, estos son más comunes que los full resolvers.

Cuando el resolver recibe una petición a la que no puede dar respuesta por si mismo, soportara dos tipos de peticiones o consultas: la consulta recursiva demanda que el servidor lance a su vez una consulta para determinar la información buscada y luego devolvérsela al cliente, la consulta interactiva implica que el servidor de nombres debería devolver la información de la que disponga además de una lista de servidores adicionales con los que el cliente puede contactar para completar su consulta.

Puede haber 4 diferentes tipos de servidor DNS:

- Servidor de nombre primario. Mantiene la base de datos de nombres y direcciones para una zona, guardando la información sobre como contactar con servidores de nombre de zonas inferiores y superiores. Tiene autoridad sobre la zona.
- Servidor de nombre secundario. Un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona de un servidor primario utilizando un proceso llamado transferencia de zona, guarda esa información en un archivo de solo lectura para aumentar la fiabilidad y descargar trabajo al DNS primario. Las transferencias de zonas realizan las actualizaciones de las bases de datos. Para permanecer sincronizados los servidores de nombres secundarios consultan a los primarios regularmente (típicamente cada tres horas) y reejecutan la transferencia de zona si el primario ha sido actualizado. Un servidor de nombres puede operar como primario o secundario para múltiples dominios, o como primario para unos y secundario para otros. Los servidores primarios o secundarios realizan todas las funciones de un servidor cache.
- Servidor de nombre maestro. Transfiere el archivo de zona a un servidor secundario.
- Servidor de nombre solo de cache. Es un servidor de nombres que no tiene autoridad para ninguna zona. Cuando un equipo solicita la resolución de un nombre al DNS primario, este servidor guarda la dirección IP que devuelve el DNS antes de enviarla al equipo solicitante, cuando se quiera consultar nuevamente ese nombre se consultara ahora al servidor de solo cache.

Todos los mensajes de DNS utilizan un único formato, Fig. 3.1.1.27.

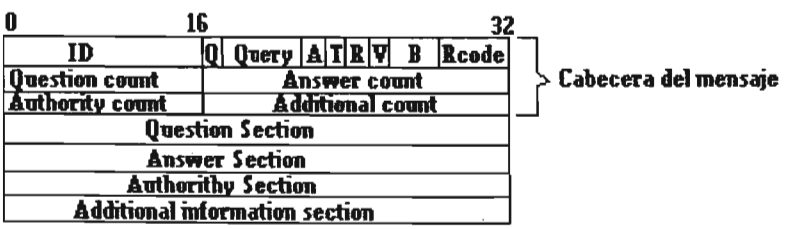


Fig. 3.1.1.27 Estructura del mensaje DNS

El resolver envía la trama al servidor de nombres. Las consultas solo utilizan la cabecera de los mensajes y una sección question. Las respuestas o retransmisiones de las consultas usan la misma trama pero con mas secciones de la misma (secciones

answer/authority/additional). La sección de cabecera siempre ha de parecer que tiene una longitud fija de 12 bytes. Las otras secciones son de longitud variable. Los campos son:

- ID: identificador de 16 bits asignado por el programa. Este ID se copia en la respuesta correspondiente del servidor de nombres y se usa para diferenciar respuestas cuando ocurren múltiples consultas, es decir correlaciona consultas y respuestas.
- Q: Bandera de 1 bit que identifica el mensaje como una consulta (0) o respuesta(1).
- Query: Campo de 4 bits que describe el tipo de mensaje:

0 Consulta estándar QUERY (nombre a dirección)
1 Consulta inversa IQUERY(dirección a nombre)
2 Petición de estado del servidor. Los demás estados son par uso futuro.

- A: Bandera de respuesta con autoridad (1 bit). Cuando es puesto a 1 identifica la respuesta como realizada por un servidor de nombre con autoridad sobre el dominio enviado en la consulta.
- T: Bandera de truncamiento (1 bit). Cuando es puesto a 1 significa que el mensaje ha sido truncado debido a que es mas largo de lo que permite el canal.
- R: Bandera de recursividad (1 bit). Indica al servidor de nombres que se requiere resolución recursiva. El bit se copia en la respuesta.
- V: Bandera de recursividad disponible (1 bit): Indica si el servidor de nombres soporta resolución recursiva.
- B: Campo de tres bits, reservado para uso futuro, debe ser cero.
- RCode: Código de respuesta. Campo de 4 bits que es establecido por el servidor de nombre para identificar el estado de la consulta:

0 No existe ningún error
1 El servidor es incapaz de interpretar la consulta debido a un error de formato.
2 El mensaje no fue procesado debido a una falla del servidor.
3 Error de nombre. El nombre de dominio en la consulta no existe. Solo es valido si el bit AA esta activo en la respuesta.
4 El Tipo de consulta no es soportada en el servidor de nombres
5 El servidor rechaza responder a la consulta por razones políticas. Los de mas valores son para uso futuro

- Question count: Campo de 16 bits que define el numero de entradas e la sección pregunta.
- Answer count: Campo de 16 bits que define el numero de recurso registrado en la sección respuesta.
- Authority count: Campo de 16 bits que define el numero de registros de recurso de nombre de servidor en la sección autoridad.
- Additional count: Campo de 16 bits que define él numero de registros de recurso en la sección de registros adicional.

Los mensajes DNS se transmiten como datagramas UDP o sobre un canal TCP, ambos por el puerto 53 del servidor. Los mensajes transportados por UDP se restringen a 512 bytes, los más largos se truncan y el bit TC de la cabecera se activa. Los mensajes transmitidos con TCP van precedidos de un campo de 2 bytes que indica la longitud total de la trama. Los servidores de nombres deben soportar ambos tipos de transporte.
Las aplicaciones de DNS usan tres utilidades comunes para consultar servidores de nombres:

- Host: Obtiene una dirección IP asociada con un nombre de host o un nombre de host asociado con una dirección IP.
- nslookup: Permite localizar información acerca de los nidos de red, examinar los contenidos de la base de datos de un servidor de nombres y establecer la accesibilidad a servidores de nombres.
- dig (Domain Internet Groper): Permite probar los servidores de nombres, reunir grandes volúmenes de información de nombres de dominio y ejecutar simples consultas de nombres de dominio.

- **NetBIOS/IP**

NetBIOS/IP es un protocolo estándar que soporta servicios NetBIOS en un ambiente TCP/IP. Soporta operaciones de Internet y red local. Varios tipos de nodo son definidos para acomodar topologías de Internet y local y permitir la operación con o sin el uso de broadcast IP. Tipos de NetBIOS pueden ser Servicio de Nombre, Sesión o datagrama. El formato del encabezado es mostrado en la Fig. 3.1.1.28

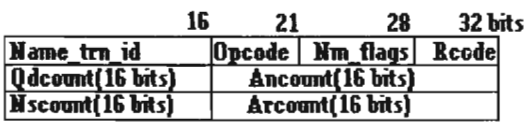


Fig. 3.1.1.28 Encabezado NetBIOS/IP

- Name_trn_id: Identificador de transacción para la transacción de servicio de nombre.
- Opcode: Paquete de tipo de código, sus valores son:

0 Consulta
1 Registro
2 Release
3 WACK
4 Refrescar

- Nm_flags: Banderas para la operación.
- Rcode: Códigos de resultado de la petición.
- Qdcount: Entero de 16 bits sin signo especificando el numero de entradas en la sección pregunta de un nombre.
- Ancount: Entero de 16 bits sin signo especificando el numero de recursos registrados en la sección respuesta de un paquete de nombre de servicio.
- Nscount: Entero de 16 bits sin signo especificando el numero de recursos registrados en la sección autoridad de un paquete de nombre de servicio.
- Arcount: Entero de 16 bits sin signo especificando el numero de recursos registrados en la sección de registros adicional de un paquete de nombre de servicio.

- **Protocolo IRC**

El protocolo de conversación en línea (Internet Relay Chat) fue desarrollado como una forma de comunicación en modo texto entre usuarios, es por si mismo un sistema de teleconferencia, el cual a través del modelo cliente-servidor, esta diseñado para ejecutarse en varias computadoras. Una instalación común involucra un solo servidor convirtiéndose en un punto central para los clientes permitiendo que los mensajes sean entregados. Sus

partes son: el servidor que brinda un punto al cual se pueden conectar los clientes para platicar entre sí y un punto para que otros servidores se conecten formando una red IRC, el cliente se conecta al servidor usando un identificador único de 9 caracteres.

- **Servidor WINS**

Microsoft desarrollo un sistema para convertir los nombres de los equipos NT en direcciones IP, el sistema es el WINS (Windows Internet Name Service). Este servidor se encarga de registrar, consultar y enviar los nombres solucionando el problema de que utilicen nombres NetBIOS en un entorno TCP/IP de forma más flexible que utilizando DNS.

- **X WINDOWS**

El sistema X-Windows es una de las interfaces gráficas de usuario GUI (Graphical User Interface) o sistema de ventanas de mapas de bits más usadas. El objeto de X_WINDOWS fue permitir al usuario controlar todas las sesiones desde una sola pantalla con aplicaciones ejecutándose ya sea en una ventana o en terminales virtuales separadas, pero con un icono en la ventana principal recordándole la existencia de esa aplicación. Se pueden gestionar tanto ventanas locales como remotas. Las ventanas remotas se establecen a través de TCP/IP y las locales mediante el uso de sockets de BSD.

El sistema X-WINDOWS se compone básicamente de dos partes que se comunican entre sí:

1.La aplicación que recibe las entradas de usuario, ejecuta un código y envía la salida al usuario. En lugar de escribir directamente en el display, la aplicación usa la interfaz de programación Xlib para enviar/recibir datos de la terminal de usuario. La parte de aplicación se conoce también como cliente X-WINDOW.

2.La terminal de usuario que ejecuta la interfaz con el display y envía o recibe datos a/de la aplicación se denomina servidor X-WINDOW.

El protocolo X-WINDOW proporciona una interfaz de ventana remota para aplicaciones de red distribuidas. Este protocolo de capa de aplicación usa protocolos TCP/IP o DECNET para el transporte.

El protocolo de conexión de redes X-WINDOW esta basado en la arquitectura cliente/servidor donde:

- El servidor es el programa de control corriendo en la estación de trabajo del usuario. Es un programa dedicado a suministrar servicios de display en una terminal grafica, a favor del usuario y a petición del cliente X-WINDOW del usuario. Controla la pantalla y maneja el teclado, el ratón y otros dispositivos de entrada para uno o más clientes X-WINDOW, también es responsable de la salida sobre el display, el mapeado de colores, la carga de fuentes y el mapeado del teclado, típicamente se ejecutan en PCs y terminales de tipo grafico, además de las terminales X-WINDOWS. Un programa de control X-server corriendo en una estación de trabajo puede simultáneamente manejar ventanas de visualización para múltiples aplicaciones, con cada aplicación actualizando asincrónicamente su ventana con información transportada por el protocolo de conexión de redes X-WINDOW.

Para proporcionar interacción del usuario con aplicaciones remotas el programa X-server corriendo en la estación de trabajo genera eventos en respuesta a la entrada de usuario tal como el movimiento del mouse o un golpe de tecla. Cuando múltiples aplicaciones se muestran, el sistema manda movimientos del mouse o clicks del ratón a la aplicación

actualmente resaltada por el apuntador del mouse. El foco de entrada actual selecciona cual aplicación recibe eventos de golpes de tecla. En ciertos casos las aplicaciones también pueden generar eventos diseccionados al programa de control X-Server.

- El cliente es una aplicación en otra parte en la red que esta diseñada para emplear una interfaz grafica de usuario para mostrar sus salidas. Típicamente muchos clientes X compiten por los servicios de un servidor X-WINDOWS, el gestor X-WINDOW resuelve los conflictos por la competencia. El gestor de X-WINDOW es un cliente X localizado en la estación de trabajo donde se ejecuta el servidor X.

El protocolo X-Window se ejecuta sobre la conexión de red y permite que se efectúen solicitudes y respuestas entre cliente y servidor. Esta orientado a conexión (usa TCP) y describe el formato de los mensajes intercambiados entre cliente y servidor sobre la conexión.

La funcionalidad del sistema X-Windows permite:

- Los servidores y clientes X-WINDOWS pueden estar en hosts diferentes. En este caso podrán usar TCP/IP para comunicarse en la red. También pueden estar en la misma maquina usando IPC (comunicación entre procesos) para comunicarse a través de sockets.
- Solo existe un servidor X por terminal con el que se pueden comunicar varios clientes, su deber es mostrar las ventanas de aplicación y enviar al cliente X las entradas de usuario.
- Depende del cliente X mantener las ventanas creadas. Los cambios efectuados en el display por otros clientes son notificados por eventos del servidor X, el cliente no se tiene que preocupar de que parte de sus ventanas son visibles o no, el servidor X lleva la cuenta de las ventanas visibles y no visibles manteniendo pilas o stacks.
- El servidor X carece de funciones de gestión, solo realiza el recorte de las ventanas sobre el puerto de visión según sus pilas. Existe un gestor de ventanas (Windows Manager) que manipula las ventanas de la cima de todos los clientes, el gestor en si es un cliente, en cuanto el gestor cambia algo en la pantalla hace que el servidor X envíe un evento a los demás clientes.

Las ventajas del sistema cliente/servidor son:

- Las aplicaciones no tienen que conocer las características hardware de la terminal y no tienen que estar en el mismo ordenador.
- Los programas Xlib son portátiles y los programadores de estos no tienen que preocuparse de las comunicaciones.
- Se pueden agregar nuevos tipos de terminal solo con proporcionar un servidor X adecuado.

Un protocolo X-Windows se puede implementar sobre cualquier mecanismo de transporte fiable y orientado a conexión. Los dsiplays se numeran siempre a partir de cero. Para conexiones TCP, el numero de display N se asocia con el puerto 5800+N y el 5900+N. El servidor X-Windows trata las conexiones en el puerto 58xx como conexiones con hosts que usan el formato ´primero el byte inferior´, y a los 59xx como aquellos que tienen el formato ´primero el byte de orden superior´.

- **SNMP.**

El crecimiento en tamaño y complejidad de las redes TCP/IP ha hecho que los mecanismos de gestión de red sean muy importantes.

La comunidad de Internet desarrolló el protocolo SNMP para permitir a diversos objetos de red participar en una arquitectura de administración de red global. Los sistemas de administración de red pueden sondear a las entidades de red implementando SNMP por información relevante a una implementación de administración de red particular. Los sistemas de administración de red aprenden de los problemas recibiendo eventos o noticias de cambio de los dispositivos de red que implementan SNMP.

El protocolo de administración de red (Simple Network Manager Protocol) se utiliza para administrar redes físicas de diferentes fabricantes, es decir, Internet, donde no existe un protocolo común en la capa de enlace, proporciona mensajes de cola y reporta problemas a través de una red hacia el administrador, usa el protocolo UDP para encapsularse y poder transportarse. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace. El formato del mensaje SNMP se muestra en la Fig. 3.1.1.29.

Fig. 3.1.1.29 Mensaje SNMP

El mensaje SNMP se compone de tres partes:

- Versión: Número de versión SNMP. Se usa para identificar el nivel de SNMP. Tanto el administrador como el agente deben usar la misma versión de SNMP. Los mensajes que contienen diferente numero de versión son descartados sin procesamiento adicional.
- Cadena de comunidad: Se usa para la seguridad, restringiendo el acceso a los datos. Es un nombre de comunidad usado para autentificar al administrador antes de permitir el acceso al agente.
- PDU: Contiene los comandos y respuestas, llamados PDU (Unidades de datos de protocolo). Existen 5 tipos diferentes comandos de PDU:
    - GetRequest: Recupera los valores de un objeto del MIB.
    - GetNextRequest: Recorre parte del MIB.
    - GetResponse: Respueta de GetRequest, GetNextRequest y SetRequest.
    - SetRequest: Altera los valores de un objeto de MIB.
    - Trap: Capacidad de los elementos de red para generar eventos como la inicialización, reinicio o fallo en el enlace. Hay siete tipos de traps: coldstart, warmstart, linkDown, linkUp, authentication failure, egpNeighborLoss y enterprise Specific.

Estándares de gestión de red

- El SMI (Structure and Identification of Management Information) define las reglas para describir los objetos gestionados y como los protocolos sometidos a la gestión pueden acceder a ellos.
- MIB (Management Information Base) define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones MIB-I y MIB-II, la primera no es recomendada.

- **Radius**

Radius es un protocolo que maneja bancos de módems y líneas seriales dispersas para números grandes de usuarios. Como los bancos de módems son un enlace al mundo externo requieren atención cuidadosa a la seguridad, autorización y la contabilización. Esto se hace manejando una sola base de datos de usuarios que permite autentificación (verificación del nombre de usuario y password) así como también la configuración de información detallando el tipo de servicio a entregar al usuario (por ejemplo SLIP, PPP, Telnet, RLogin). Las características clave de Radius son:

- Se basa en el modelo cliente/servidor.
- Usado para la seguridad de red.
- Posee mecanismos de autentificación flexible.
- Es un protocolo extensible.

El encabezado Radius se observa en la Fig. 3.1.1.30

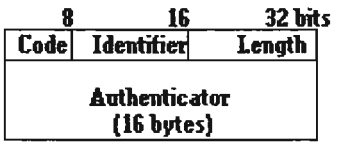


Fig. 3.1.1.30 Encabezado Radius

- Code: Tipo de mensaje.
- Identifier: Hace corresponder peticiones y respuestas.
- Length: La longitud del mensaje incluyendo el encabezado.
- Authenticator: Un campo usado para autentificar la respuesta desde el servidor radius y en el algoritmo de ocultamiento de password.

- **Protocolo TACACS+**

El protocolo TACACS+ (Terminal Access Controller Access Control System) proporciona control de acceso para routers, servidores de acceso a la red y otros dispositivos de computación en red vía uno o más servidores centralizados. Proporciona servicios de autentificación, autorización y contabilización separados. El encabezado se puede observar en la Fig. 3.1.1.31.

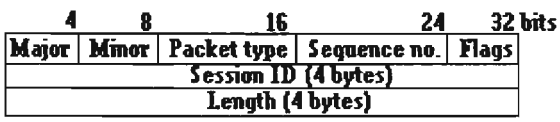


Fig. 3.1.1.31 Encabezado del protocolo TACACS+

- Major versión: El numero de versión mayor TACACS+.
- Minor versión. El número de versión menor. Esto es implementado para permitir se realicen revisiones al protocolo mientras se mantiene la compatibilidad con versiones anteriores.
- Packet type: Los tipos de paquete pueden ser:

TAC_PLUS_AUTHEN :=0x01 (Autentificación)
TAC_PLUS_AUTHOR :=0x02 (Authorization)
TAC_PLUS_ACCT:=0x03 (Accounting)

- Sequence number: Numero de secuencia del paquete actual para la sesión actual. El primer paquete TACACS+ en una sesión debe tener el numero de secuencia 1 y

cada paquete subsecuente incrementara el numero de secuencia en 1. Así los clientes solamente mandan paquetes que contienen números de secuencia impar y los demonios TACACS+ solamente mandan paquetes que contienen números de secuencia par.
- Flags. Contiene varias banderas en la forma de mapas de bits. Los valores de la bandera significan si el paquete es encriptado.
- Session ID: El identificador para esta sesión TACACS+.
- Length: La longitud total del cuerpo del paquete TACACS+ (no incluido el encabezado).

- **Kerberos**

El sistema de autentificación y autorización kerberos es un sistema de seguridad basado en la encriptación que proporciona autentificación mutua entre usuarios y servidores en un entorno de red. Las metas del sistema son:
- Autentificación para evitar solicitudes/respuestas fraudulentas entre servidores y usuarios que debe ser de índole confidencial.
- Cada servicio puede implementar su propio sistema de autorización independientemente de la autentificación.
- Permitir la contabilización integrada segura y fiable con estructura modular y soporte para la facturación.

El protocolo de seguridad Kerberos es de los mas seguros por lo cual es muy ampliamente utilizado para este fin. El protocolo utiliza una aplicación especial llamada servidor de autenticidad para validar las contraseñas y esquemas de encriptado.
El proceso de autentificación en el sistema kerberos se realiza de la siguiente forma:
El cliente que desea contactar con un servidor para que le dé un servicio, debe pedir primero un ticket de una tercera parte de mutua confianza, el KAS (Kerberos Authentication Server). Este ticket se obtiene como una función en la que uno de los componentes es una llave privada conocida solo por el servicio y el KAS de forma que el servicio puede estar seguro de que el ticket procede solo de kerberos. El KAS conoce al cliente por su nombre principal. La llave privada k(c) es la llave de autentificación conocida solo por el usuario y el KAS. El proceso de autentificación consiste en el intercambio de los siguientes cinco mensajes:
1 Cliente -> KAS: El cliente envía un mensaje al KAS para solicitarle un ticket el cual usara con el servidor de tickets (TGS).
2 KAS->Cliente: El servidor de autentificación busca el nombre del cliente (c) y el nombre del servicio (TGS, servicio de tickets) en la base de datos de kerberos y obtiene una llave de encriptación para cada uno de ellos k(c) y k(TGS). A continuación crea una respuesta para enviarla al cliente, la cual contiene el ticket inicial que garantiza el acceso al servidor solicitado. También genera una llave aleatoria de encriptación llamada llave de sesión. Luego encripta el ticket usando la llave de encriptación y se crea el mensaje con el ticket sellado y la llave de sesión.
3 Cliente -> TGS: cuado recibe el mensaje el cliente lo desencripta usando su llave secreta k(c) que solo el y el KAS conocen. Comprueba que el nounce coincide con la solicitud especifica y guarda la llave de sesión para futuras comunicaciones con el TGS. El cliente envía un mensaje al TGS que contiene el ticket inicial, el nombre del servidor, un nounce y un nuevo identificador que lleva un sello de tiempo.

4 TGS -> Cliente: El TGS recibe el mensaje del cliente y descifra el ticket sellado usando su llave de encriptación TGS. EL TGS obtienen la llave de sesión para TGS del ticket descifrado y la emplea a su vez para descifrar el autentificador sellado. Finalmente checa la hora actual en el autentificador para cerciorarse de que el mensaje es reciente. Ahora el TGS busca el nombre del servidor que aparece en el mensaje en su base de datos de kerberos y obtiene la llave de encriptación para el servicio. El TGS crea una nueva llave aleatoria de sesión para el cliente y el servidor para generar un nuevo ticket, luego ensambla un nuevo ticket y lo envía al cliente.
5 Cliente -> Servidor: El cliente recibe el mensaje y lo descifra con la llave de sesión para el TGS. De este mensaje calcula una nueva llave de sesión. El cliente construye un autentificador y lo sella con la nueva llave de sesión. Por ultimo envía un mensaje que contiene el ticket sellado y el autentificador al servidor para solicitar su servicio.
El servidor recibe el mensaje y descifra primero el ticket sellado con su llave de encriptación, luego usa la llave de sesión del ticket para descifrar el autentificador y realiza el proceso de validación. Una vez que el servidor ha validado al cliente, el cliente tiene la opción de validar a su vez al servidor para evitar que un intruso suplante al servidor. El cliente requiere que el servidor le devuelva un mensaje con el sello de tiempo.
En resumen los puntos centrales del esquema kerberos son:

- Para que cada estación emplee cualquier servidor requiere un ticket. Los tickets se obtiene del TGS. El primer ticket es especial ya que es para el propio TGS y se obtiene del KAS.
- Cada ticket esta asociado con una llave de sesión que se asigna cada vez que se concede un ticket.
- Los tickets son reutilizables pues tienen un tiempo de vida de alrededor de ocho horas. Después de que un ticket ha expirado, el usuario ha de identificarse de nuevo al kerberos, introduciendo el nombre de usuario y el password.
- Cada vez que un cliente inicia conexión con el servidor hace falta un nuevo autentificador. El autentificador contiene un sello de tiempo que expira a los pocos minutos de haber sido expedido por lo que los relojes de clientes y servidores deben estar sincronizados.
- El servidor debería mantener un seguimiento de solicitudes anteriores de los clientes para las que el sello del tiempo en el identificador aun es valido. Así puede rechazar solicitudes duplicadas que pueden surgir de un ticket y un identificador robados.

- **Protocolo REXEC**

REXECD (Remote EXEcution Command Daemon) es un servidor que permite la ejecución del comando REXEC o RSH (Remote SHell Protocol) desde un host remoto sobre la red TCP/IP. La función del cliente es realizada por el proceso REXEC.
REXECD es un servidor tipo daemon que maneja comandos lanzados por host remotos y transfiere ordenes a maquinas virtuales que actúan como esclavos para la ejecución de tareas. El daemon realiza un login automático así como la autentificación cuando el usuario introduce su identificador y password.
El comando REXEC se usa para definir el identificador de usuario, el password, dirección del host, y el proceso a iniciar en el host remoto. Tanto el servidor como el host están conectados sobre la red TCP/IP.

- **RPC**

RPC (Remote Procedure Call) es un estándar desarrollado por Sun Microsystems. Es una interfaz de programación de aplicación para el desarrollo de aplicaciones distribuidas. Permite que los programas llamen a subrutinas que se ejecutan en un sistema remoto. Este concepto se simplifica de la siguiente forma: El programa llamador o cliente envía un mensaje de llamada al proceso servidor y espera por un mensaje de respuesta. En el lado servidor un proceso permanece a la espera de mensajes de llamada. Cuando llega una llamada el proceso servidor extrae los parámetros de procedimiento, calcula los resultados y los devuelve en un mensaje de respuesta.
El protocolo RPC se puede implementar sobre cualquier protocolo de transporte ya sea TCP o UDP. Los mensajes de llamada y respuesta se formatean al estándar XDR. El mensaje de llamada RPC consta de varios campos:
- Números de programa y de procedimiento con tres campos que identifican univocamente al procedimiento a ejecutar:
    - Numero del programa remoto.
    - Numero de versión del programa remoto.
    - Numero del procedimiento remoto.

Cada programa remoto esta conectado a un puerto el cual se elige libremente exceptuando los puertos bien conocidos.
- Campos de autentificación, compuesto por dos campos, credenciales y verificador. Cada implementación es libre de elegir entre los varios protocolos de autentificación que están soportados. Algunos son:
    - Autenticación nula.
    - Autenticación UNIX.
    - Autenticación DES. Además del identificador de usuario, al servidor se le envía un campo correspondiente a un sello de tiempo.. Este sello de tiempo es la hora actual, cifrada con una llave conocida por el servidor y el llamador (se basa en el concepto de llave secreta y llave publica de DES).

- Parámetros de los procedimientos. Son los datos pasados al procedimiento remoto.

3.2 IP

El conjunto de protocolos TCP/IP son la base del funcionamiento de la red mundial Internet, todos y cada uno de los protocolos que componen a la pila TCP/IP a poyan o soportan el funcionamiento de la Internet y la innumerable cantidad de aplicaciones que corren sobre ella. De todo ese conjunto de protocolos dos son los que se distinguen por su importancia y por que dan el nombre al conjunto de protocolos de Internet, estos dos protocolos son el protocolo TCP y el protocolo IP. De estos dos, el protocolo IP ha tomado todavía mayor importancia por que el funcionamiento real de Internet se implementa usando este protocolo, es decir la transmisión de información en Internet se realiza a través del protocolo IP, por lo que actualmente se cuenta con un gran numero de aplicaciones que funcionan sobre IP.

3.2.1 Que es el protocolo de Internet IP

El protocolo de Internet IP (Internet Protocol) es uno de los protocolos que constituyen la pila de protocolos TCP/IP, este protocolo trabaja en la capa de Internet del modelo TCP/IP.
IP es el principal protocolo de capa de red y de la suite de protocolos de Internet. Junto con el protocolo de control de transmisión TCP, IP representa el corazón de los protocolos de Internet. Tiene dos responsabilidades principales: proporcionar entrega de datagramas con el mejor esfuerzo sin conexión, a través de la conexión de redes y proporcionar fragmentación y reensamblado de datagramas para soportar enlaces con tamaños de MTUs diferentes.
En el modelo OSI, IP es un protocolo de capa de red (capa 3) que contiene información de direccionamiento y algo de información de control que permite a los paquetes ser ruteados.
Este protocolo oculta la red física subyacente creando una vista de red virtual. A su vez permite a los protocolos superiores y al de transporte olvidarse de la forma de enviar los paquetes de información por la red.
IP es el protocolo universal responsable del envío y enrutamiento de paquetes y permite que cualquier computadora en cualquier parte del mundo se pueda comunicar en cualquier momento con cualquier otra computadora en cualquier parte del mundo.
El protocolo IP es la base de toda comunicación en la red de redes o Internet, ya que es el protocolo que permite la transmisión de datos por y entre las redes.
La unidad de información intercambiada por IP se conoce como datagrama. El datagrama contiene un encabezado y un área de datos. El área de datos no es especificada ya que puede ser utilizada arbitrariamente por el protocolo de transporte.
El protocolo IP es el software que implementa el mecanismo de entrega de paquetes sin realizar una conexión previa por lo que los datagramas viajan de extremo a extremo de la red, sin la confianza de que los datos lleguen a su destino, sin control de flujo ni recuperación de errores asume pocas cosas solo que los datagramas probablemente serán transportados al host destino. Los paquetes de información que IP envía por la red son tratados independientemente pudiendo viajar por diferentes trayectorias para llegar a su destino por lo que se pueden perder, desordenar o incluso duplicarse sin que IP maneje estas situaciones, estos servicios dependen de los protocolos superiores, la responsabilidad

de arreglar estas situaciones IP se las deja al nivel TCP, por lo anterior se dice que IP usa la técnica del mejor esfuerzo.
El protocolo de Internet envía los paquetes de la capa de transporte (también conocidos como Unidades de datos del protocolo de transporte TPDU) a través de Internet. IP fragmenta los TPDUs en partes pequeñas y las reensambla en el host destino o en una estación intermedia. A cada fragmento o TPDU le adapta un encabezado IP.
IP básicamente se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir por donde se deben encaminar los datagramas salientes pudiendo levar a cabo labores de fragmentación intencional para permitir que un nodo con un buffer limitado pueda transportar todo el datagrama y es responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen.
El protocolo IP es un protocolo que trabaja a través de direcciones IP, asigna una sola dirección IP a cada host, los hosts pueden ser, computadoras, ruteadores, servidores, impresoras y cualquier equipo que pueda trabajar en red. Cada uno de estos hosts debe tener una sola dirección IP para que de esta forma puedan conectarse y compartir los recursos de la red.
La importancia del protocolo IP esta en su capacidad de direccionamiento lógico, el cual representa el lenguaje mas utilizado para la interconexión de ambientes heterogéneos.
El protocolo IP también define la ruta inicial por la que serán mandados los datos. Si el protocolo IP identifica una dirección destino como una dirección local envía el paquete directamente a la maquina. Si el destino es identificado como un destino remoto, IP checa sus tablas de rutas. Si encuentra una ruta envía el paquete usando esa ruta de lo contrario envía el paquete al gateway (router) por defecto.
IP maneja tablas de ruteo para tomar la decisión de la ruta a seguir de entre las varias que puede haber entre el host fuente y el host destino a lo largo de Internet. Aunque los fragmentos pueden llegar fuera de orden IP los reensambla en secuencia.
IP es un protocolo sin conexión. Esta basado en la idea de los datagramas interred, que son transportados transparentemente pero no siempre con seguridad desde el host fuente hasta el host destino, quizás recorriendo varias redes mientras viaja.
El protocolo IP trabaja de la siguiente forma:
La capa de transporte toma los mensajes y los divide en datagramas de hasta 64000 octetos cada uno. Cada datagrama se transmite a través de la red Internet posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final cuando todas las piezas llegan a la maquina destino, la capa de transporte los reensambla para así reconstruir el mensaje original. Un datagrama consta de una parte de cabecera y una parte de datos. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable.
Cuando los datagramas viajan de un equipo a otro pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra dependiendo del medio físico empleado para la transmisión. El tamaño máximo de los paquetes mencionado es el MTU (Maximum Transmisión Unit) y ninguna red puede transmitir un paquete de tamaño mayor a este MTU.

3.2.2 Protocolos IP

Algunos protocolos que trabajan muy estrechamente con IP en el nivel de Internet de TCP/IP son los siguientes:

- **Protocolo ARP.**

Es un protocolo que se encarga de convertir las direcciones IP en direcciones de red física. Cuando un paquete llega a una red local mediante el ruteo IP, la entrega de ese paquete al host destino se debe realizar forzosamente mediante la dirección MAC del mismo (los hosts individuales en una sola red física se conocen en la red a través de su dirección física o MAC que es el numero de la tarjeta de red) por lo que se tiene que convertir la dirección IP destino del paquete en la dirección MAC equivalente. Esto es por que las direcciones Ethernet y las direcciones IP son dos números distintos que no guardan ninguna relación entre ellos. De esta labor se encarga el protocolo ARP.
El protocolo de resolución de direcciones ARP (Address Resolution Protocol) es uno de los protocolos que opera en los niveles más bajos del conjunto TCP/IP, se usa en redes de difusión. ARP convierte las direcciones IP en direcciones de red física o Ethernet (MAC de 48 bits) para que puedan ser utilizados por los controladores. Mediante este protocolo una estación (generalmente un router) obtiene la dirección MAC a partir de la dirección IP lanzando un broadcast, el broadcast se realiza mandando un mensaje o petición ARP a todas las demás estaciones, para que la estación que tiene la dirección IP conteste con un mensaje de respuesta ARP en el que envía su dirección física MAC (la dirección MAC es la que se encuentra grabada en la tarjeta de interfaz de red, compuesta de 48 bits, de los cuales 24 identifican al fabricante y los otros 24 es el numero de serie único universalmente asignado a cada interfaz de red), esta información es almacenada en las tablas de direcciones MAC de los equipos (a veces de conocen como cache ARP). Cada host posee una tabla ARP de correspondencias entre la dirección física con la dirección IP. Los protocolos TCP/IP direccionan los hosts mediante las direcciones IP, pero al mandar un datagrama a su destino es necesario conocer la dirección física.
Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un router) y el dispositivo hardware al que se deberá enviar si es una red 802.3/4/5 se consulta el modulo ARP, Fig.3.2.2.1, para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

Encabezado de capa física		**n bytes**
espacio de dirección de hardware		**2 bytes**
espacio de dirección de protocolo		**2 bytes**
dirección de hardware longitud en bytes (n)	**dirección de protocolo longitud en bytes (n)**	**2 bytes**
código de operación		**2 bytes**
dirección de hardware origen		**n bytes**
dirección de protocolo origen		**n bytes**
dirección de hardware destino		**n bytes**
dirección de protocolo destino		**n bytes**

Fig. 3.2.2.1 Paquete de petición /respuesta ARP

Significado de los campos

- Espacio de dirección de hardware: Especifica el tipo de hardware, por ejemplo Ethernet.
- Espacio de dirección de protocolo: Especifica el tipo de protocolo, el mismo que el campo tipo EtherType en la cabecera de IEEE802.
- Longitud de la dirección de hardware: Especifica la longitud en bytes de la dirección hardware del paquete. Para IEEE 802.3/5 será de 6.
- Longitud de la dirección de protocolo: Especifica la longitud en bytes de las direcciones del protocolo en el paquete. Para IP será 4.
- Código de operación: Especifica si se trata de una petición (1) o una solicitud (2) ARP.
- Dirección de hardware fuente/destino: Contiene las direcciones físicas de hardware. En IEEE 802.3 son direcciones de 48 bits.
- Dirección de protocolo fuente/destino: Contiene las direcciones del protocolo. En TCP/IP son direcciones de 32 bits.

El modulo ARP intenta hallar la dirección en su cache. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits y realiza la transmisión. Si no la encuentra descarta el paquete (ya que el protocolo de alto nivel lo vuelve a transmitir) y genera un broadcast a toda la red mediante una petición ARP con los campos de la Fig. 3.2.2.2

Fig. 3.2.2.2 Petición ARP

Para el paquete de solicitud la dirección de hardware destino es el único campo indefinido del paquete.

Si una maquina en la red reconoce su propia dirección IP en la petición devolverá una respuesta ARP al host que la solicito con los campos de la Fig. 3.2.2.3, la respuesta contendrá la dirección física del hardware así como información de encaminamiento.

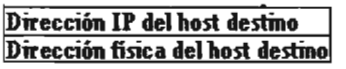


Fig.3.2.2.3 Respuesta ARP

La dirección física recibida se agrega a la tabla ARP. Una vez que la maquina que realiza la petición tiene el dato de la dirección física destino envía los paquetes al host destino usando la dirección física obtenida.

ARP se diseño apara para usarse en redes que soportan broadcast por hardware, por lo que se emplea en redes IEEE 802, además en las DIX Ethernet para mapear las direcciones IP a dirección hardware.

- **Protocolo RARP.**

Protocolo usado en la incialización delas computadoras para que una vez que envian su dirección física obtengan de un servidor RARP su dirección IP correspondiente.

Este es otro de los protocolos que trabajan en el nivel mas bajo de TCP/IP, RARP (Reverse Address Resolution Protocol) es usado al arranque de una estación para que esta envíe un mensaje con su dirección física MAC para obtener de un servidor RARP su dirección IP

correspondiente en una red de difusión. El formato de sus paquetes es el mismo de ARP, cuando un host desea conocer su dirección IP difunde un paquete por la red que contiene su dirección física. El servidor RARP al recibir el paquete busca en su tabla RARP la dirección correspondiente la dirección física y le envía la respuesta al host origen con su dirección. Una vez obtenida la dirección IP la guarda en memoria y no vuelve a usar RARP hasta que no se inicia de nuevo. Este protocolo es poco usual, ya que se usan más los protocolos BOOTP y el DHCP.

- **Protocolo ICMP.**

El protocolo de mensajes de control y error de Internet (Internet Control Message Protocol) es un protocolo de mantenimiento y gestión de la red que ayuda a supervisar la red, así como encontrar la ruta optima de transmisión para los datagramas. El protocolo ICMP tiene su propio numero de protocolo (numero 1) que lo habilita para utilizar el IP directamente. También proporciona información de error o control entre nodos, a través de mensajes generados por TCP/IP y no por el usuario. Los cuatro mensajes que puede generar son: destino no alcanzable (Destination Unreacheable), control de congestión (Flow Control), redireccionamiento (Redirecting Destination) y tiempo excedido (Time Out). Por los mensajes que puede manejar su utilidad consiste en controlar si un paquete no puede alcanzar su destino, si su tiempo de vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Los mensajes de control y error que maneja informan a la fuente para que evite o corrija el problema detectado.
La utilidad de diagnostico PING (Protocol Internetwork Group) hace uso de este protocolo para diagnosticar si una estación esta conectada a la red.
Los mensajes ICMP se envían en datagramas IP. La cabecera IP siempre tendrá un numero de protocolo de 1, indicando que se trata de ICMP y un servicio de tipo 0 (rutina). El campo de datos IP contendrá él autentico mensaje ICMP en el formato mostrado en la Fig. 3.2.2.4

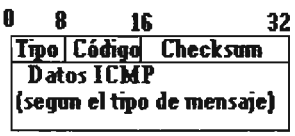


Fig. 3.2.2.4 Formato del mensaje ICMP

Los campos son:

- Tipo: Especifica el tipo de mensaje que puede ser:
  - Destino no alcanzable (Destination unreachable). El router envía este mensaje si la distancia a la red es infinita o no puede enviar el datagrama al destino por cualquier motivo. El host envía este mensaje si el protocolo de nivel superior o el puerto especificado no están activos en el host.
  - Control de congestión (flow control). Cuando los buffer del host destino se llenan al 80%, este envía el mensaje al host origen indicándole esto para que disminuya la velocidad de envío de los mensajes.
  - Redireccionamiento (Redirection). El router envía este mensaje al host emisor para indicarle que el mensaje IP se enviara por otro router con una ruta mas optima.
  - Tiempo excedido (timeout). Mensaje que envía el router cuando el campo TTL del datagrama IP es cero o si el temporizador de reensamblado expira antes de que se reciban todos los fragmentos del datagrama inicial.

- Petición/respuesta de eco. Mensajes que utiliza la utilería PING para comprobar que el enlace funciona correctamente.

Estos tipos de mensaje se muestran en la tabla 3.2.2.1

Tipos de mensaje ICMP	
Tipo	Tipo de mensaje
0	Respuesta de eco (echo reply)
3	Destino inalcanzable (Destination unreachable)
4	Origen saturado (Source quench)
5	Redirección (cambiar ruta-redirect)
8	Solicitud de eco (echo)
11	Tiempo excedido para un datagrama (time exceded)
12	Problema de parámetros en un datagrama (parameter problem)
13	Solicitud de fecha y hora (timestamp request)
14	Respuesta de fecha y hora (timestamp reply)
17	Solicitud de mascara de dirección (address mask request)
18	Respuesta de mascara de dirección (address mask reply)

Tabla 3.2.2.1 Tipos de mensaje ICMP

Una breve explicación de estos mensajes es

- Destination unreachable (3).

Si este mensaje se recibe de un router, intermedio, significa que el router considera la dirección IP destino inalcanzable. Si se recibe de un host destino, significa que el protocolo especificado en el campo de número de protocolo del datagrama original no esta activo en ese host, o el puerto indicado no esta activo.

Si un router implementa el protocolo de resolución de caminos MTU, el formato del mensaje Destination unreachable se cambia por el código 4 para incluir el MTU del enlace que no pudo aceptar el datagrama.

- Source quench (4).

Es usado por un router intermedio para informar que no dispone de suficiente espacio en el buffer para encolar los datagramas de salida para la siguiente red. Un host usa este mensaje para informar que los datagramas entrantes llegan demasiado rápido para ser procesados.

- Redirect (5).

Un router intermedio usa este mensaje para informar que el host debería enviar los datagramas a un router cuya dirección se especifica en el mensaje ICMP. Este router habrá de estar en la misma subred que el host que envío el datagrama y el que lo devolvió. Enviara el datagrama a su siguiente dirección de salto, si la dirección del router coincide con la dirección fuente del datagrama original, indica un bucle. La cabecera ICMP tendrá uno de los siguientes valores:

0 Network redirect.
1 Host redirect.
2 Network redirect for this type of service.
3 Host redirect for this type of service.

- Echo (8) y echo reply (0)

Echo es usado para detectar si un host esta activo en la red. Un host puede comprobar si otro host esta activo mandando una solicitud de eco. La fuente inicializa el identificador y numero de secuencia, añade algunos datos al campo de datos y envía el echo ICMP al host de destino. El receptor cambia el tipo de mensaje a echo reply y devuelve el datagrama al host fuente. Este mecanismo es empleado por el comando o aplicación PING para determinar si es posible alcanzar un host de destino, PING encapsula la solicitud de eco (tipo 8) en un datagrama IP y lo manda a la dirección IP..

- Router advertisement (9) y Router Solicitation (10).

Estos dos mensajes se usan si un host o un router soporta el RDP (Router Discovery Protocol). El uso de multicast es recomendado, pero se puede usar el broadcast si la interfaz no soporta el multicast. Los router anuncian periódicamente sus direcciones IP en subredes si han sido configurados para que lo hagan. Los anuncios se hacen en la dirección de multicast (224.0.0.1) o de broadcast limitado (255.255.255.255). Por default se envían anuncios con un tiempo de vida TTL de 1800 seg. (30min.). Los routers responden a los mensajes de solicitud, respondiendo directamente al solicitante, o esperando un tiempo aleatorio y corto para responder con un multicast. Los hosts pueden enviar solicitudes hasta que reciben una respuesta. Las solicitudes se envían a la dirección de multicast para todos los routers (224.0.0.2) o a la de broadcast limitado (255.255.255.255).

- Time exceded (11).

Un router intermedio usa este mensaje para indicar que el tiempo de vida (TTL) de un datagrama IP ha expirado. Si un host de destino lo usa significa que el TTL para ensamblar el datagrama ha expirado mientras el host esperaba uno de sus fragmentos. La cabecera ICMP puede tener uno de los siguientes valores:

0 Transit TTL exceeded.
1 Reassembly TTL exceeded.

- Parameter problem (12).

El campo puntero apunta al byte del datagrama original en el que se encontraron problemas en el procesamiento de los parámetros de la cabecera IP. La cabecera ICMP puede tomar unos de los siguientes valores:

0 Unspecified error.
1 required option missing.

- Timestamp request (13) y timestamp reply (14).

Estos dos mensajes se usan para medir el rendimiento y para depuración, no se usan para sincronizar, para eso esta el NTP (Network Time Protocol). Para ello el host fuente envía el identificador y numero de secuencia, fija su sello de tiempo y se lo envía al receptor. El host receptor fija el valor de los sellos de tiempo de recepción y envío, cambia el tipo de mensaje a (timestamp reply) y se lo devuelve al receptor. El receptor dispone de dos sellos de tiempo en caso de que haya una diferencia sensible entre los tiempos de recepción y transmisión. Los sellos de tiempo indican el número de milisegundos transcurridos desde la medianoche según el meridiano de Greenwich (GMT)

- Información request (15) e Information Reply (16).

Un host lanza el mensaje Information request para obtener una dirección IP de la red a la que esta conectado y espera una respuesta del servidor autorizado para asignar direcciones IP. La respuesta contendrá las direcciones IP de red en los campos de dirección fuente y de dirección destino de la cabecera IP. Este mecanismo es obsoleto por otros protocolos como RARP.

- Address Mask (17) y Address Mask Reply (18).

Un host usa el mensaje Address mask request cuando quiere determinar que mascara de subred usa la red a la que esta conectado. Para obtener una mascara de subred, el host hace un broadcast del mensaje address mask request. Cualquier host que se haya configurado para enviar mensajes address mask reply rellenara esta mascara, convertirá el tipo de mensaje a address mask reply y se lo devolverá al host fuente.

- Código. Contiene el código de error que afecta al datagrama al que se refiere el mensaje IP. La interpretación depende del tipo de mensaje.

Si un gateway no puede enviar un datagrama a la dirección destino, manda un mensaje de error ICMP al origen. El valor del campo tipo es 3 y el tipo de error viene dado por el campo código, tabla 3.2.2.2

Código	Descripción
0	Red no alcanzable (network unreachable)
1	Host no alcanzable (host unreachable)
2	Protocolo no alcanzable (protocolo unreachable)
3	Puerto no alcanzable (port unreachable)
4	Necesaria fragmentación con la opción DF (Fragmentation needed but the Do Not Fragmentation bit was set)
5	Fallo de la ruta de origen (source route failed)
6	Red de destino desconocida (destination network unknown)
7	Host de destino desconocido (destination host unknown)
8	Fallo del host de origen (source host isolated)
9	Red prohibida administrativamente (Destination Network Administratively Prohibited)
10	Host prohibido administrativamente (Destination Host Administratively Prohibited)
11	Tipo de servicio de red no alcanzable (network unreachable For this type of service)
12	Tipo de servicio de host no alcanzable (host unreachable For this type of service)
13	Comunicación prohibida administrativamente por filtración (Communication administratively prohibited by filtering)
14	Violación del host de prioridad (host precedence violation)
15	Prioridad de desconexión en efecto (precedence cutoff in effect)

Tabla 3.2.2.2 Significado de los códigos de inalcanzable

Cuando el buffer del receptor se llena al 50% este controla el flujo con un mensaje de tipo 4 código 0.

Cuando la ruta por defecto no es la mas adecuada el gateway puede enviar un mensaje ICMP de direccionamiento que contiene la ruta correcta, el mensaje será del tipo 5 y con código entre 1 y 3.

Para prevenir loops el datagrama IP contiene un tiempo de vida. Conforme pasa por cada gateway este valor es decrementado en 1, cuando este valor llega a 0 el gateway manda un

mensaje de error ICMP y descarta el datagrama, el mensaje es del tipo 11 y con código igual a 0.
Cuando un datagrama es mal construido o es dañado, el gateway manda un mensaje de error al origen y descarta el datagrama, el mensaje es tipo 12 y código 0.

- Checksum. Contiene el complemento a 1 de 16 bits de la suma del mensaje ICMP comenzando desde el campo tipo.
- Datos ICMP. Contiene información para el mensaje ICMP. Normalmente contiene una parte del mensaje IP original para el que se genero el mensaje ICMP.

Cuando un router o host de destino debe informar al host fuente acerca del procesamiento de datagramas, utiliza ICMP, el cual tiene las siguientes características:

- ICMP se comporta como si fuera un protocolo de nivel superior al usar IP (ya que los mensajes ICMP se encapsulan en los datagramas IP). Sin embargo ICMP es parte integral de IP.
- ICMP no hace fiable a IP, ya que solo informa de algunos errores. Aun con ICMP puede ocurrir que los datagramas no se entreguen y que no se informe de su perdida.
- ICMP puede informar de errores en cualquier datagrama IP con la excepción de mensajes IP. Para evitar repeticiones infinitas.
- Para datagramas IP fragmentados, los mensajes ICMP solo se envían para errores ocurridos en el fragmento cero, nunca se refieren a un datagrama con un campo de desplazamiento de fragmento.
- Los mensajes ICMP nunca se envían en respuesta a datagramas con una dirección IP de destino que sea de broadcast o de multicast.
- Los mensajes ICMP nunca se envían en respuesta a un datagrama que no tenga una dirección IP de origen que represente a un único host. Es decir la dirección de origen no puede ser cero, una dirección de loopback, de broadcast o de multicast.
- Los mensajes ICMP nunca se envían en respuesta a mensajes ICMP de error. Se pueden enviar en respuesta a consultas (mensajes 0, 8, 9, 10 y 13 al 18).
- Los mensajes ICMP pueden ser generados para informar de errores mas no debe ser obligatorio que se generen.

El PING y Traceroute son dos aplicaciones que usan ICMP. El PING usa los mensajes Echo y Echo Reply para determinar si un host es alcanzable. El traceroute envía datagramas IP con bajos TTLs para que expiren durante la ruta que les dirige al destino. Usa los valores de los mensajes ICMP Time Exceded par determinar en que parte de la red expiraron los datagramas y reconstruye un esquema de la ruta hasta el host de destino.

3.2.3 Versiones de IP

IPv4

Actualmente toda la infraestructura instalada de Internet trabaja con IPv4, esta versión desde su creación suscito muchas discusiones sobre el formato de su cabecera, en la actualidad enfrenta el problema de la capacidad de direccionamiento. La capacidad de direccionamiento mediante 32 bits permite $4x10^9$ direcciones que en un principio se suponía suficiente, ya que eran muy pocas las computadoras que se tenían por área de empresas, escuelas y hogares. Hoy en día se ha quedado corto con el crecimiento explosivo

de Internet, y el gran numero de computadoras y equipos que manejan aplicaciones sobre IP y que necesitan tener conexión directa a través de Internet con el extremo que desean comunicarse, sobre todo por que un gran numero de direcciones son desperdiciadas por el ineficiente mecanismo de asignación y la mala administración que se realiza de dichas direcciones. El aumento todavía mayor de las maquinas conectadas en red y dispositivos electrónicos que ofrecen servicios de Internet en dispositivos de comunicación móvil va agravar todavía mas este problema.

El aumento cada vez mayor de las tablas de ruteo de Internet es otro problema que se tiene con IP. El ruteo en una gran red debe ser jerárquico con una profundidad igual a la amplitud de la red. El ruteo IP es jerárquico a tres niveles: red, subred y maquinas. Los ruteadores de las grandes redes de interconexión deben tener una entrada en sus tablas de ruteo para todas las redes IP existentes.

Limitaciones de IPv4.

Internet creció rápidamente en los últimos años, por ejemplo a principios de 1995 se tenían mas de 32000 redes que conectaban mas de 3.8 millones de maquinas en mas de 90 países. Como una dirección de 32 bits proporciona unos 4 billones de posibles direcciones, parecería que el esquema de direccionamiento es suficiente para todos los hosts de Internet puesto que parece que aun es posible un incremento en mil veces la ocupación del espacio de direcciones. Pero esto no es posible entre otras causas por que:

- Las direcciones de 32 bits de IPv4 que están en uso desde 1970 no fueron diseñadas para abastecer el grado de uso del Internet de hoy aunado a que su asignación ha sido deficiente y restrictiva por lo que son difíciles de obtener y tienden a agotarse en un futuro muy cercano restringiendo el uso de Internet para los nuevos usuarios e incluso para los ya existentes forzándolos a usar direcciones privadas.
- La dirección IP se divide en un numero de red y en una parte local administrada por separado. Aunque el espacio de direcciones dentro de una red puede estar poco ocupado, en lo que respecta al espacio efectivo, si se usa un numero de red, todas las direcciones de esa red están ocupadas.
- Las direcciones se estructuran en las clases A, B y C de distintos tamaños y deben considerarse por separado los espacios de cada una.
- El modelo de direccionamiento IP requiere que todas las redes IP tengan números unívocos, estén o no conectadas a Internet.
- El crecimiento explosivo de TCPIP en ciertas áreas como la difusión para interconectar terminales de venta o receptores de televisión por cable incrementaría enormemente él numero de hosts IP. Debido al gran numero de usuarios de Internet, dispositivos como los teléfonos de 3G que hacen uso de IP móvil, aplicaciones y protocolos (VoIP, Videoconferencia, juegos en línea, IPsec, kerberos) que necesitan direcciones IP que sean de alcance global, únicas y ruteables se necesitan mas direcciones.
- Mobile IP es uno de los tópicos que vienen empujando mas fuerte la implementación de una nueva versión de direccionamiento debido a que necesita que ambos extremos de una sesión TCP mantengan la misma dirección IP por todo el tiempo que dure la sesión (home address usada para la conexión de extremo a extremo).
- El modelo actual de direccionamiento IP con una sola dirección para cada host podría cambiar en el futuro.

- Las tablas de ruteo de Internet ya son muy grandes debido a que su crecimiento ha sido exponencial.
- También se necesita cambiar la dirección cuando un nodo de red se mueve a un nuevo lugar en la red (care-of address mediante la autoconfiguración de la dirección usada para el ruteo).
- El IP actual no tiene un solo estándar para seguridad.
- La administración del sistema en el IP actual es una labor ardua, compleja, lenta, propensa a errores y las redes de suscriptores no pueden ser dinámicamente renumeradas.

Estos factores hacen que el espacio de direcciones este muy reducido. El problema del agotamiento de las direcciones IP es el problema principal que enfrenta IPv4. Aunque actualmente se aplican algunos métodos o técnicas que tratan de aliviar el problema o prolongar el agotamiento como:

- El uso de medidas intermedias como las direcciones privadas disminuye el desempeño de la red al tener que usar la técnica NAT (Network Address Translation) lo que provoca que se rompa el esquema de las aplicaciones que usan el direccionamiento de extremo a extremo.
- El ruteo con CIDR han facilitado la disminución de las tablas de ruteo pero es una solución para corto tiempo.

La primera idea es corregir el sistema de direcciones que es demasiado rígido. Actualmente pueden estar conectados unos 16 millones de maquinas de la clase A, mas de 65000 de la clase B y 254 de la clase A. Las clases A y B están casi agotadas y si una empresa desea conectar 500 maquinas deberá conseguir dos direcciones con lo que su red se encontrara segmentada y las tablas de ruteo sobre Internet sobrecargadas. Actualmente este problema es parcialmente resuelto con supernetting CIDR que permite redistribuir una parte de las direcciones subutilizadas.

Al final el espacio actual terminara por agotarse. Las estimaciones fijan el agotamiento del espacio de direcciones entre el 2005 y el 2011. Antes de que esto ocurra hará falta un sustituto para la versión actual de IP.

El IETF creo el grupo de trabajo IPng cuya tarea inicial era encontrar una solución a la ineficiencia de las direcciones IP de 32 bits por ser inapropiadas para la identificación lógica de los equipos de terminales y la estructura de la jerarquía (redes y subredes).

Entre los requerimientos que debería cumplir la nueva versión de IP están:

- El espacio de direcciones debería ser mucho más grande, esto permitiría una reducción en el uso de las direcciones IP y dejaría el espacio de direcciones poco poblado permitiendo que las nuevas direcciones estén mas estructuradas que en IPv4.
- El nuevo protocolo debería permitir la encapsulación de sus propios paquetes y los de otros protocolos.
- La nueva versión debería añadir clases de servicio para distinguir los tipos de datos transmitidos, tales como trafico isócrono como audio y video en tiempo real.
- Debería permitir proporcionar un direccionamiento multicast de forma que este mas integrado con el resto de la pila que IPv4.
- Debería proporcionar autentificación y encriptación.
- Debería mantener las virtudes de IPv4 como su robustez, independencia de las características de la red física, alto rendimiento, topología flexible, extensibilidad,

servicio de datagramas, direccionamiento univoco a nivel global, protocolo de control integrado y estándares de libre distribución.

- La implementación debería realizarse mediante una transición sencilla y paulatina.
- La nueva versión debería coexistir con IPv4.

Las causas de los problemas actuales de IPv4 y los trabajos realizados para buscar una solución a esos problemas han propiciado la creación de un nuevo sistema o versión de IP (IPv6).

IPv6

Ya existe una nueva versión del protocolo de Internet IP que recibe el nombre de IPv6 (Internet Protocol versión 6). IPv6 es una versión actualizada del protocolo de Internet IPv4.

Diferentes grupos han elaborado propuestas para diseñar la nueva versión de IP:

- Una primer propuesta era reemplazar IP por el protocolo CLNP (Connectionless Network Protocol) del servicio de red OSI conocido como TUBA (TCP and UDP over Bigger Addresses) el cual permitía la convergencia de OSI e Internet.
- Otras propuestas que rebatían a TUBA presentaron propuestas como IP sobre IP, SIP (Simple IP) y PIP (Paul´s Internet Protocol). SIP proponía aumentar el tamaño de las direcciones IP y PIP proponía una estrategia de ruteo más innovadora que permitiese una implementación eficaz de encaminamiento prioritario y que facilitase la movilidad.
- Las propuestas de SIP y PIP se fusionaron para generar SIPP (Simple IP plus) que intentaba preservar tanto la eficacia de las codificaciones de SIP como la potencia de las técnicas de ruteo de PIP.

El IETF opto por tomar la propuesta SIPP como base IPng con algunas modificaciones para tener en cuenta las cualidades de otras propuestas. De esta forma SIPP conserva las direcciones IPv4 de tamaño fijo pero más grandes que pasan de 8 a 16 bytes, permite autoconfiguración de direcciones suprime campos con semántica mal diseñada o que nunca fueron usados y añade otros. Los campos no concernientes a los ruteadores (información de fragmentación, autentificación, etc.) están colocados después de la cabecera principal en unas cabeceras de extensión, el tipo de servicio es cambiado en beneficio de la etiqueta de flujo. La fragmentación de ahora en adelante será efectuada únicamente por los nodos terminales. Tendrá soporte a la función de movilidad y source routing.

El IETF realizó la propuesta de una nueva versión de IP, el IPv6 que fue diseñada para ser un paso evolutivo de IPv4. Esta nueva versión permite extender la capacidad de direccionamiento del nivel de red de IPv4 que puede ser instalado como un software normal con características mejoradas en dispositivos Internet debiendo poder operar con IPv4.

IPv6 se diseño para funcionar bien en redes de alto rendimiento como ATM y al mismo tiempo se diseño para ser eficiente en redes de poco ancho de banda. Proporciona adicionalmente una plataforma para nuevas funcionalidades de Internet que pudieran requerirse en el futuro.

IPv6 se ha diseñado para solucionar todos los problemas que surgen con la versión anterior y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.). Aunque los cambios que se introducen en esta nueva versión son muchos y de gran importancia la transición desde la versión 4 no debería ser problemática debido a

las características de compatibilidad que se han incluido en el protocolo y como una condición cuando se diseño dicho protocolo.
Algunas de las especificaciones de IPv6 son:

- Se compone de estándares abiertos y accesibles.
- El método de transición es claro y realista.
- Permite la gestión de por lo menos mil millones de redes, es decir $1x10^{12}$ estaciones con autoconfiguración de las direcciones y puesta en marcha de un direccionamiento global y único de cada equipo.
- Utiliza los métodos de ruteo RIP, OSPF, etc.
- Es independiente de la red física. La etiqueta de flujo (Flow Label) aun debe corresponder con los circuitos virtuales ATM.
- Soporta las diversas topologías de redes interconectadas y un servicio no orientado a conexión (servicio de datagramas).
- Garantiza la seguridad de ciertas operaciones como la autentificación o la criptografia especifica del nivel 3 de red.
- Soporta la difusión de grupo (multicast).
- Gestiona varias clases de servicio con la etiqueta de flujo.
- Incorpora protocolos equivalentes a los presentes en IPv4 como Ping, traceroute, ICMP, etc.
- Permite la encapsulación de diversos protocolos en IPv6.
- Posee suficientes direcciones para permitir la conexión a Internet de los mas de 2 billones de dispositivos móviles existentes.
- Ofrece las características necesarias para la conexión de redes (internetworking) móviles.

3.3 IPv4

En temas anteriores hemos visto el protocolo IP a grandes rasgos en este tema veremos temas como sus características, formato del encabezado del datagrama IP, direcciones IPv4, clases de direcciones, ruteo. entraremos en poco mas de detalle de este protocolo para conocer mas acerca del protocolo IP en su versión 4,

3.3.1 Características del protocolo IPv4

En el tema 3.2 definimos lo que es el protocolo IP, por lo que aquí solo se mencionan algunas de sus características:

- El protocolo IP se implementa en software.
- Datagramas. IP define la unidad básica para la transferencia de datos en una interred como datagramas, especificando el formato exacto de un datagrama IP.
- Protocolo de entrega de datagramas. Es un protocolo que realiza la trasmisión de la información que le llega de las capas superiores en unidades llamadas datagramas desde el origen hasta el destino.
- Protocolo best effort. Realiza el mejor esfuerzo (best effort) para la transmisión y entrega de paquetes.
- Proporciona servicios sin conexión. IP realiza la transmisión de los datagramas sin establecer una conexión previa (protocolo no orientado a conexión). Es no orientado a conexión ya que antes de enviar los datos no establece ni se mantiene una conexión lógica en el nivel Internet entre los extremos para realizar la transferencia de información, simplemente manda la información con su debida información de direccionamiento para tener una forma de determinar como llegar al destino.
- Proporciona un servicio no confiable. Es protocolo no confiable, por lo que no garantiza el control de flujo, no garantiza la recuperación de errores y no garantiza la entrega de paquetes, es decir no hay seguridad de que los datos lleguen a su destino. Es no confiable ya que al enviar los datagramas no cuenta con mecanismos de verificación de entrega (envío de paquetes sin secuencia) y de comprobación de errores (envío de paquetes sin recibir reconocimientos), ni control de congestión. No garantiza la entrega en secuencia de los datagramas enviados, por que los primeros datagramas se pueden retrasar respecto a los que se enviaron atrás de ellos, en general los paquetes se pueden perder, duplicar, demorar, o entregar en diferente orden. También no se garantiza la entrega por que los datagramas se pueden enrutar de manera incorrecta o se pueden mutilar al dividir y reensamblar los fragmentos del mensaje. Estas tareas de control de secuencia, recepción y verificación de datagramas enviados a través de la red son dejadas a cargo de los protocolos de la capa superior o capa de transporte.
- Checksum. Para detectar errores de transmisión solo realiza la suma de verificación al encabezado del datagrama, no realiza una suma de verificación para el contenido de datos del datagrama.
- Fragmentación y reensamblado. IP realiza la fragmentación y reensamblado de datagramas si es necesario. Al atravesar diferentes redes la longitud de los paquetes puede variar por lo que se establece un tamaño máximo permitido en cada red lo

que se conoce como MTU (Maximum Transmissión Unit) que es de aproximadamente 1500 bytes, si el paquete excede este tamaño se debe fragmentar o reensamblar según la dirección de transmisión. Los ruteadores o hosts de reenvío realizan las tareas de fragmentación de los datos en unidades de trasferencia de datos llamados datagramas, esta fragmentación puede ocurrir múltiples veces. El host de destino vuelve a reensamblar fragmentos para formar los paquetes de datos originales.

- Direcciones IP. IP Trabaja a través de una sola dirección que se asigna unívocamente al host. Realiza un direccionamiento lógico mediante direcciones lógicas IP de longitud fija de 32 bits.
- Ruteo. IP define las reglas de procesamiento de paquetes. Implementa funciones de ruteo para determinar la trayectoria mas optima a seguir por el datagrama. Usa un proceso de ruteo para direccionar y reenviar paquetes. El mecanismo de ruteo de los datagramas determina las trayectorias que deben seguir los datagramas para llegar a su destino. El ruteo lo realiza paso a paso por todos los nodos en el camino del datagrama o mediante rutas estáticas o dinámicas.
- IP es un protocolo ruteado ya que es capaz de proporcionar la información y los medios para hacer que un mensaje o datagrama llegue a su destino final.
- Define las reglas para que los host y routers procesen paquetes, los descarten o generen mensajes de error.
- Los datagramas IP tienen un formato que se constituyen con una cabecera y los datos del usuario. La cabecera contiene información para el nivel IP, esa información contiene los datos necesarios para enrutar los datagramas y los datos de usuario contienen la información o paquetes que le llegan de los niveles superiores. Los datagramas a su vez son encapsulados en tramas de longitud de terminada por la red física.
- Protocolo independiente del nivel de interfaz de red. IP es independiente de las tecnologías de red, es decir es independiente de los atributos del nivel físico de OSI como el cableado, señalización y velocidad y es independiente del nivel de enlace de OSI como los esquemas de control de acceso al medio, direccionamiento y tamaño máximo de trama. Su direccionamiento de 32 bits es independiente del direccionamiento a nivel de enlace.
- Protocolo de interconexión (internetworking). IP es un protocolo de interconexión ruteable, ya que al contener la cabecera del datagrama las direcciones IP origen y destino, y al componerse cada una de esas direcciones con la dirección de red y la dirección de host, es posible la entrega de datagramas entre redes o enrutamiento, además IP permite la interconexión de dos o más redes mediante enrutadores de IP.
- Tecnología de conmutación de paquetes. En una tecnología de conmutación de paquetes cada paquete se reenvía por los conmutadores de la red de conmutación mediante un esquema de direcciones con significado global. En el caso de IP los paquetes son los datagramas (mensaje sin secuencia ni reconocimiento), los conmutadores son los ruteadores IP y el direccionamiento con significado global con las direcciones IP de destino. La dirección de destino se examina en cada ruteador y el ruteador toma la desición de ruteo independiente y reenvía el paquete.

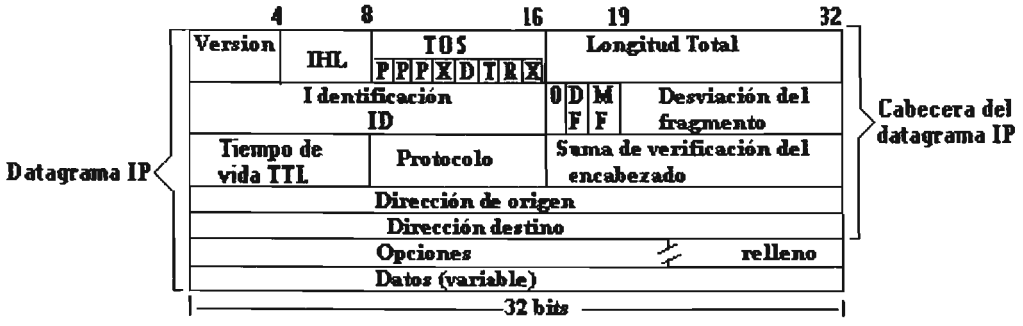
- Si un paquete no es recibido este permanecerá en la red durante un tiempo finito, ya que el encabezado de IP contiene un contador de saltos que se usa para limitar el numero de enlaces por los que puede viajar un paquete antes de descartarlo..
- El tamaño máximo del datagrama IP es de 65635 bytes.

3.3.2 Formato de los datagramas IPv4

El protocolo IP proporciona el servicio de transmisión de datagramas en la capa de Internet del modelo TCP/IP. Todos los protocolos dentro de la suite excepto ARP y RARP usan IP para rutear datagramas tramas de host a host.
La misión de IP es encaminar el datagrama que le llega del protocolo superior sea TCP o UDP, encamina el datagrama sin comprobar la integridad de la información que contiene.
El datagrama es la unidad básica usada por el protocolo IP para organizar los datos a transmitir entre maquinas que se comunican mediante el protocolo IP
Un datagrama se forma mediante una cabecera que se antepone a la cabecera del protocolo de nivel superior, al cual le sigue el conjunto de datos de información provenientes del protocolo que hace uso de IP, así se forma el datagrama que se tiene que enrutar. Si llego un paquete de información del protocolo TCP la estructura del datagrama seria como muestra la Fig. 3.3.2.1

Fig. 3.3.2.1 Datagrama IP

Los datagramas IP contienen una cabecera con información para el nivel IP (información de ruteo e información de control asociada con la entrega de datagramas) y datos (Cabecera TCP o UDP mas los datos propios del protocolo que hace uso de IP) relevantes para los protocolos superiores.
Estos datagramas a su vez cuando son usados en un ambiente de red LAN se encapsulan en tramas que dependiendo de la red física tienen una longitud determinada. Para el caso de Ethernet la longitud máxima es de 1500 bytes.
La cabecera del datagrama IP es de al menos 20 bytes y esta formada por varios campos (al menos 12) como se muestra en la Fig. 3.3.2.2



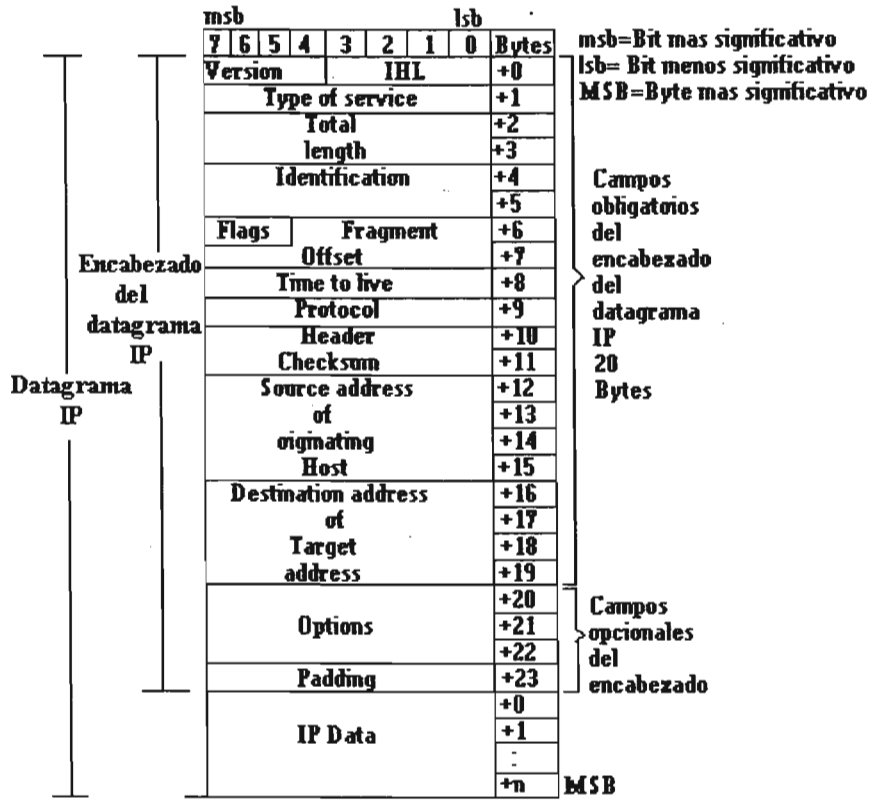


Fig. 3.3.2.2 Formato del datagrama IP

En la Fig. 3.3.2.2 tenemos dos formas diferentes de ver el datagrama de IP. Los significados de los campos del datagrama IPv4 son:

- Versión:

Indica la versión del protocolo IP que se esta usando para crear el datagrama. Este campo permite que diferentes versiones del protocolo IP puedan operar en la Internet. La versión actual en uso es IPv4. La 5 es experimental y la 6 es la de próxima generación. El tamaño del campo es de 4 bits.

- Longitud de la cabecera (IHL):

Debido a que la longitud de la cabecera no es constante el campo IHL (Internet Header Length) indica la longitud de la cabecera IP en palabras de 32 bits, es decir indica cuantos grupos de 32 bits componen la cabecera. El valor de la longitud mínima de la cabecera IP es de 5 palabras de 32 bits correspondientes a 160 bits=20 bytes. El tamaño del campo es de 4 bits.

- Tipo de servicio (TOS):

Es un campo de 8 bits que permite al host indicarle a la subred la calidad de servicio esperado por este datagrama para entrega a través de los routers en la red IP así como la precedencia y las prioridades o importancia de los datos que se envían. Las redes pueden ofrecer precedencia de servicio, lo que significa que solamente pueden aceptar trafico sobre

una cierta precedencia en horas de mucha carga. Hay un regateo de tres vías entre bajo retardo, alta confiabilidad y alto rendimiento.
Se compone de dos subcampos, Fig. 3.3.2.3:

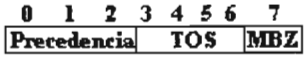


Fig. 3.3.2.3 Subcampos del campo TOS

- Los tres bits mas altos (del 0 al 2 de izquierda a derecha) indican la precedencia que es una medida de la naturaleza y prioridad de este datagrama en niveles del 0 al 7 como muestra la tabla 3.3.2.1.

Bits 0-2	Nivel de precedencia
000	Rutina
001	Prioridad
010	Inmediato
011	Flash
100	Ignorar flash
101	Critico/ECP
110	Control de red (Control de internetwork)
111	Control de red (Network Control)

Tabla 3.3.2.1 Tabla de niveles de precedencia del campo TOS

- Los cinco bits siguientes indican el tipo de servicio. Normalmente no son usados pero algunas aplicaciones como el control de encaminamiento y los algoritmos de encolamiento si los usan. El bit D se usa para manejar el retardo (delay). El bit T se usa para manejar el rendimiento total (throughput). El bit R maneja la confiabilidad de que se dañe o pierda el datagrama, tabla 3.3.2.2

Bit	Tipo de servicio	Valor del bit	
		0	1
3 (1000)	Maneja el retardo (Delay)	Retardo normal	Bajo retardo
4 (0100)	Maneja el rendimiento (Throughput)	Rendimiento normal	Alto rendimiento
5 (0010)	Maneja la confiabilidad (Reliability)	Confiabilidad normal	Alta confiabilidad
6 (0001)	Minimiza el costo monetario		
7	Reservados para uso Futuro.	Debe ser cero	

Tabla 3.3.2.2 Tipos de servicio

Estos tres bits son muy usados por el protocolo OSPF. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Por ejemplo para voz digitalizada es más importante la entrega rápida que corregir errores de transmisión. En tanto que para la transferencia de archivos es más importante tener una transmisión confiable que la entrega rápida.

- Longitud:

Indica la longitud total en bytes del datagrama completo, incluida la cabecera del datagrama IP y los datos. Como este campo usa 16 bits el tamaño máximo del datagrama no podrá ser mayor de 65536 bytes, aunque en la practica este valor será mucho más pequeño ya que datagramas tan grandes son imprácticos para la mayoría de los hosts y redes. Todos los hosts deben estar preparados para aceptar datagramas de hasta 576 bytes independientemente de sí llegan completos o en fragmentos. Es recomendable que los hosts manden datagramas más grandes de 576 bytes solo si el destino esta preparado para aceptar los datagramas más grandes. Tamaño del campo es de 16 bits.

- Identificación (ID):

Determina si el paquete es un fragmento o un datagrama. Este campo le pone un identificador (numero secuencial entre 0 y 65535) a este paquete. Cuando se produce la fragmentación de un datagrama, a todos los fragmentos en que se divide el datagrama se les asigna el mismo identificador. De esta manera el receptor puede identificar a que datagrama pertenece el fragmento recién llegado para proceder a su reensamblado. El tamaño del campo es de 16 bits.

- Apuntadores (flags):

Banderas de control de fragmentación. Cuando un datagrama excede el tamaño del MTU se debe fragmentar. Los bits de este campo son usados para control, para indicar si se permite o no la fragmentación, Fig. 3.3.2.4.

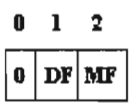


Fig.3.3.2.4 Bits de control de fragmentación

El bit 0 esta reservado y debe tener un valor de cero.
Dos bits se usan para indicar el proceso, el bit DF (Don´t Fragment bit +7) es usado por el servidor origen para indicar que no se puede fragmentar el paquete, cuando este bit toma un valor diferente de 0 y la longitud de un datagrama excede el MTU será una orden para que los gateways no fragmenten el datagrama por que el extremo destino es incapaz de ensamblar los fragmentos, si el datagrama no puede pasarse a través de una red se deberá encaminar sobre otra red o desecharse y un mensaje de error es enviado al host origen por medio del protocolo ICMP.
Bit 1. Bit de no fragmentar DF (Don´t fragment) :

- 0 Se permite la fragmentación.
- 1 No se permite la fragmentación.

Si se permite la fragmentación el bit MF (More Fragment) se usa para indicar que hay mas fragmentos si esta encendido, si esta apagado indica que este es él ultimo fragmento, todos los fragmentos con excepción del último deberán tener este bit encendido ya que verifica que no falten fragmentos para que el datagrama se reensamble por completo.
Bit 2 : Bit de mas fragmentos MF (More fragments) :

- 0 Indica que es él ultimo fragmento.
- 1 Indica que no es él ultimo y que hay mas fragmentos.

El tamaño del campo es de 3 bits.

- Desviación de fragmento (fragment offset):

Se usa para recomponer los datagramas previamente fragmentados. Los bits de este campo se emplean como contadores de desplazamiento para indicar la posición (offset) en bytes de cada fragmento respecto al datagrama original. Esta expresado en grupos de 8 bytes (64 bits) ya que en un datagrama todos los fragmentos con excepción del ultimo deberán ser un múltiplo de 8 octetos que es la unidad elemental de fragmentación. Como se proporcionan 13 bits hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65536 octetos que coinciden con el campo longitud total. El campo de offset se va incrementando en cada fragmento del datagrama que s envía empezando con cero. Si el paquete no estuviera fragmentado este campo tendría un valor de cero. El tamaño del campo es de 13 bits.

- Tiempo de vida:

El tiempo de vida TTL (Time To Live) del datagrama, es un contador que se utiliza para limitar el tiempo de vida de los paquetes por lo que especifica en segundos el tiempo que puede viajar por la red un datagrama. El tiempo de vida esta limitado a 255 segundos, el numero recomendado para IP es 64. Cada vez que un datagrama pasa por un ruteador resta de este campo el tiempo que tarda en procesar el datagrama (mínimo 1 aunque el tiempo de proceso sea menor). Cuando este campo llega a cero antes de alcanzar su destino se supone que el datagrama esta atrapado en un bucle infinito y debe destruirse. El originador del datagrama manda un mensaje ICMP cuando el datagrama es descartado. La intención es causar que los datagramas que no puedan ser entregados se descarten y limitar el máximo tiempo de vida del datagrama. Debido a que el tiempo de proceso de cada router de un datagrama es menor a 1 segundo y de cualquier modo tiene que restarle 1 al valor TTL este campo se convierte en un indicador del numero de saltos que tiene permitido el paquete. Se permiten 15 saltos y 31 interfaces, al salto 16 se descarta el paquete. El valor inicial lo debería fijar el protocolo superior que crea el datagrama. Tamaño del campo es de 8 bits.

- Protocolo:

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitara saber que hacer con él. El numero usado en este campo sirve para indicar a que protocolo o proceso de transporte pertenece el datagrama que se encuentra después de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Puede identificar hasta 255 protocolos de la capa de transporte. Especifica el formato del área de datos. Algunos de los protocolos superiores importantes que puede manejar se listan en la tabla 3.3.2.3. Tamaño del campo es de 8 bits:

Numero de protocolo	Keyword	Protocolo
0		Resevado
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway to Gateway Protocol
4	IP	IP In IP Encapsulation
5	ST	Stream
6	TCP	Transmission Control protocol
8	EGP	Exterior Gateway Protocol
9	IGP	Private Interior Gateway Protocol
17	UDP	User Datagram Protocol
29	ISO-TP4	ISO Transport Protocol Class 4
35	IDRP	Inter-Domain Policy Routing Protocol
41	SIP	Simple Internet Protocol
50	SIPP-ESP	SIPP Encapsulation Security Payload
51	SIPP-AH	SIPP Authentication Header
80	ISO-IP	ISO Internet Protocol
88	IGRP	IGRP
89	OSPFIGP	OSPF (Open Shortest Path First) IGP
101-254		No asignado
255		Reservado

Tabla 3.3.2.3 Números de los protocolos de nivel superior asignados

- Checksum:

Este campo indica el valor de la suma de comprobación (checksum). La suma de verificación se aplica solamente a los campos de la cabecera IP incluido el mismo checksum (cuyo valor es cero para efectos de calculo) y no a los datos. Este valor es resultado del complemento a uno de la suma (en complemento a uno) de todos los bits que componen la cabecera. Esta suma es necesaria ya que proporciona la seguridad de que los datos contenidos en la cabecera IP son correctos, es decir no están dañados ni modificados. El checksum se recalcula en cada nodo por el que pasa el datagrama antes de reenviarse, ya que al atravesar los distintos gateways el campo TTL va variando. Por razones de eficiencia este campo no puede usarse para comprobar los datos incluidos después de la cabecera IP para evitar errores. Los usuarios de IP en el cuerpo del mensaje IP deberán incluir su comprobación a partir del campo de checksum de la cabecera encapsulada en el datagrama IP y que corresponde al nivel de transporte. Si el checksum de la cabecera no se corresponde con los contenidos el datagrama se desecha ya que al menos un bit de la cabecera esta corrupto y el datagrama podría haber llegado al destino equivocado. Tamaño del campo es de 16 bits.

- Dirección origen:

Almacena la dirección IP del host origen del paquete. Tamaño de campo es de 32 bits.

- Dirección destino:

Almacena la dirección IP del host destino del paquete. Tamaño del campo es de 32 bits.

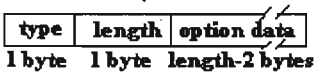
Una distinción es realizada entre nombres, direcciones y rutas. Un nombre indica un objeto a ser visto. Una dirección indica la localización del objeto. Una ruta indica como llegar al objeto. El protocolo de Internet trata primeramente con direcciones. Es tarea de los protocolos de nivel mas alto (tal como host-a-host o aplicación) hacer el mapeo de nombres a direcciones. El modulo de Internet mapea direcciones Internet a direcciones de red local. Es tarea de los procedimientos de mas bajo nivel (tal como red local o gateways) hacer el mapeo de direcciones de red local a rutas.

- Opciones:

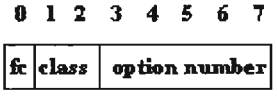
Un múltiplo de 32 bits es usado para almacenar las opciones IP, este campo es de longitud variable y es determinado por la longitud de la cabecera, puede haber cero o más opciones.
Las opciones pueden o no aparecer en los datagramas. Deben ser implementadas por todos los módulos IP (hosts y gateways). Lo que es opcional es su transmisión en cualquier datagrama particular no su implementación, esto es no se requieren que todas las implementaciones IP sean capaces de generar opciones en los datagramas que crean pero si que sean capaces de procesar datagramas que contengan opciones. En algunos ambientes la opción seguridad puede ser requerida en todos los datagramas.
Este campo proporciona un espacio para permitir que versiones subsiguientes de los protocolos incluyan información que actualmente no esta presente en el diseño original y para evitar asignar bits de cabecera a información que muy rara vez se necesita. Auque un host no esta obligado a poner opciones, puede aceptar y procesar opciones recibidas en un datagrama.
Puede haber dos formatos para las opciones que dependen del valor del numero de opción hallado en el primer byte.

- Un byte de tipo (type byte).

- Un byte de tipo, un byte de longitud y uno o más bytes de opciones.



El byte de tipo (type) tiene la misma estructura en ambos casos:



Cada octeto esta formado por los campos Copia, Clase de opción y Numero de Opción.

- El bit 1 que es el campo de bandera de copia fc (flag copy) se usa cuándo un datagrama va a ser fragmentado y viaja a través de nodos y gateways, entonces la opción es copiada en todos los fragmentos. Cuando tiene un valor fc=1 (copiada) las opciones son las mismas para todos los fragmentos, pero si toma el valor fc=0 (No copiada) las opciones son eliminadas.

- Clase de opción es un campo de 2 bits que cuando tiene valor 0 (control) indica datagrama o control de red; cuando tiene valor 2, indica depuración o mediciones. Los valores 1 y 3 son reservados para uso futuro.
- El número de opción (5 bits) indica una acción especifica. La implementación IP procesa datagramas que contienen opciones como:

- Opción de seguridad. Esta opción es usada por aplicaciones seguras.
- Opción de ruta prefijada. En el campo options se especifica una lista de direcciones Internet que componen el camino que deberá seguir el datagrama.
- Opción de registrar la ruta. El host fuente crea una lista vacía de direcciones Internet en el campo options y cada maquina que manipula el datagrama ha de grabar su dirección en esta lista.
- Opción de registrar la hora. Cada maquina graba la hora en la que manipulo el datagrama y opcionalmente graba también su dirección.
- Otras opciones mas pueden ser informe de errores, depuración, sellado de tiempo.

La tabla 3.3.2.4 muestra las características de las opciones IP

Clase de opción	Numero De opción	Octetos	Descripción
0	0	1	Fin de alineación
0	1	1	Para alinear dentro de una lista de opciones
0	2	11	Seguridad (aplicaciones militares)
0	3	Variable	Ruteo del origen
0	7	Variable	Grabar/trazar ruta
0	9	Variable	Ruteo estricto del origen
2	4	Variable	Fecha y hora de Internet

Tabla 3.3.2.4 Características de las opciones IP

Donde:

- 0 Fin de la lista con class a cero, fc a cero y sin byte de longitud o de datos. Solo se requiere si la longitud de la cabecera IP (que es un múltiplo de 4 bytes) no se corresponde con la longitud real de las opciones.
- 1 No operación, tiene class a cero, fc a cero y no hay byte de longitud ni de datagramas. Se puede usar para alinear campos en el datagrama.
- 2 Seguridad. Tiene class a cero, fc a 1 y el byte de longitud a 11 y el de datos a 8. Se usa para la información de seguridad que necesitan las especificaciones del departamento de defensa de EU.
- 3 LSR (Loose Source Routing). Tiene class a cero, fc a uno y hay un campo de datos de longitud variable.
- 4 IT (Internet Timestamp). Tiene class a 2, fc a cero y hay un campo de datos de longitud variable.
- 7 RR (Record Route). Tiene class a cero, fc a cero y hay un campo de datos de longitud variable.
- 8 SID (Stream ID o identificador de flujo). Tiene class a cero, fc a uno y hay un byte de longitud a cuatro y un byte de datos. Se usa con el sistema SATNET.

- 9 SSS (Strict Source Routing). Tiene class a cero, fc a uno y hay un campo de datos de longitud variable.

- Length:

Cuenta la longitud en bytes de la opción, incluyendo los campos de tipo y de longitud.
Option data. No contiene datos relevantes para la opción.
El campo opciones tiene una longitud variable puede haber cero o más opciones. Si las opciones IP no utilizan los 32 bits se rellenan con bits adicionales a ceros para que la longitud de la cabecera IP sea un numero entero de palabras de 32 bits.

Opciones de encaminamiento del datagrama IP
En el campo opciones del datagrama IP se tienen dos opciones para que el emisor proporcione información explicita de ruteo y una opción para que el datagrama determine la ruta que va a emplear.
Las dos opciones de información de ruteo son:

- LSR (Loose Source Routing)

  Esta opción también conocida como LSRR (Loose Source and Record Route) permite que la fuente suministre información de ruteo explicita que usaran los routers que retransmitirán el datagrama e información para grabar la ruta seguida por el datagrama. Las partes de esta opción son los de la Fig. 3.3.2.5:

Fig. 3.3.2.5 Opción LSR

  Donde:

  - 1000001 El valor 131 decimal es el valor del byte option para LSR.
  - Length. Contiene la longitud de este campo incluyendo los campos type y length.
  - Pointer. Apunta a los datagramas de la opción en la siguiente dirección IP a procesar. Si su valor supera la longitud de la opción se alcanza el final de la ruta de la fuente y el resto del ruteo se ha de basar en la dirección IP de destino (como sucede en los datagramas que no tienen esta opción).
  - Route data. Es una serie de direcciones de 32 bits.

Cuando un datagrama llega a su destino y la ruta de la fuente no esta vacía (el valor del pointer es menor que el valor de length), entonces el receptor:

- Tomara la siguiente dirección IP de este campo (el indicado por pointer y lo pondrá en el campo de la dirección IP de destino del datagrama).
- Pondrá la dirección IP local (dirección de la red por la que se enviara el datagrama) en la SL (Source List) en la localización a la que apunte el valor pointer.
- Incrementara el pointer en 4.
- Transmitirá el datagrama a la nueva dirección IP de destino.

Este procedimiento asegura que la ruta de retorno se graba en route datagram (en orden inverso) de modo que el receptor use estos datagramas para construir un LSR en el sentido inverso. Se llama LSR (loose source route) por que al router retransmisor se le permite usar cualquier ruta y cualquier numero de host intermedios para alcanzar la siguiente dirección de la ruta.

Aquí hay que hacer notar que el emisor pone la dirección IP del primer router intermedio en el campo dirección IP destino y las direcciones de los demas routers de la ruta, incluyendo el destino en la opción source router. La ruta que hay grabada en el datagrama cuando este llega al objetivo contiene las direcciones IP de cada uno de los routers que retransmitió el datagrama.

- SSR (Strict Source Routing)

Esta opción también se conoce como SSRR (Strict Source and Record Route) usa el mismo principio que LSR solo que el router intermedio debe enviar el datagrama a la siguiente dirección IP en la ruta especificada por la fuente a través de una red conectada directamente y no por un router intermedio. Si no puede hacerlo se envía un mensaje ICMP "Destination Unreachable".

El formato de esta opción es el de la Fig. 3.3.2.6:

Fig. 3.3.2.6 Opción SSR

Donde:

- 1001010. Es el valor en decimal 137 del byte option para el método SSR.
- Length. Contiene la longitud de este campo incluyendo los campos type y length.
- Pointer. Apunta a los datagramas de la opción en la siguiente dirección IP a procesar. Si su valor supera la longitud de la opción se alcanza el final de la ruta de la fuente y el resto del ruteo se ha de basar en la dirección IP de destino (como sucede en los datagramas que no tienen esta opción).
- Rote data. Es una serie de direcciones IP.

La opción para determinación de ruta es:

RR (Record Route)

Esta opción proporciona un medio para grabar la ruta de un datagrama IP. Su funcionamiento es de forma parecida al SSR, pero en este caso el host fuente deja el campo de datos de ruteo vacío que sé ira llenando a medida que el datagrama viaja. El host fuente debe dejar suficiente espacio para esta información: si el campo se llena antes de que el datagrama llegue a su destino, el datagrama se retransmitirá, pero se dejara de grabar la ruta. El formato de esta opción es mostrado en la Fig. 3.3.2.7:

Fig. 3.3.2.7 Opción RR

Donde:

- 00000111. Es el valor 7 en decimal del byte option para el método RR.
- Length. Contiene la longitud de este campo incluyendo los campos type y length.
- Pointer. Apunta a los datagramas de la opción en la siguiente dirección IP a procesar. Si su valor supera la longitud de la opción se alcanza el final de la ruta de la fuente y el resto del ruteo se ha de basar en la dirección IP de destino (como sucede en los datagramas que no tienen esta opción).

Opción IT (Internet Timestamp)
El sello de tiempo (timestamp) es una opción para forzar a algunos o a todos los routers de la ruta hacia el destino a poner un timestamp en los datos de la opción. Este valor se mide en segundos y se puede usar para la depuración. El formato de la opción es mostrado en la Fig. 3.3.2.8:

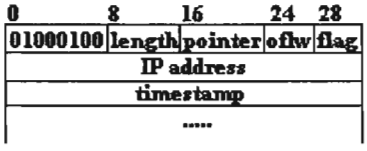


Fig. 3.3.2.8 Opcion IT

Donde:

- 01000100. Es el valor 68 en decimal del byte option para IT.
- Length . Contiene la longitud total de esta opción, incluyendo los campos type y length.
- Pointer. Apunta al siguiente timestamp a procesar (el primero disponible).
- Oflw. El campo sobreflujo (overflow) es un entero sin signo de 4 bits que indica él numero de módulos IP que no pueden registrar timestamps por falta de espacio en el campo datos.
- Flag. Valor de 4 bits que indica como se han de registrar los timestamps. Sus valores posibles son:

0 Solo timestamps almacenados en palabras consecutivas de 32 bits.
1 Cada timestamp se precede con la dirección IP del modulo que efectúa el registro.
2 La dirección IP sé preespecifica, y un modulo IP solo realiza el registro cuando encuentra su propia dirección en al lista.

- Timestamp. Un timestamp de 32 bits medido en milisegundos desde la medianoche según GMT.

El host emisor debe componer esta opción con un área de datos lo bastante grande para almacenar todos los timestamps.

- Padding:

El campo padding son bits de relleno. Cuando se utilizan opciones en el campo options los datagramas se rellenan con bits a cero. Se usan de 1 a 3 octetos puestos a cero si es necesario para hacer que él número total de octetos en la cabecera sea divisible por cuatro.

- Datos:

En este campo están los datos contenidos en el datagrama que pasan al protocolo superior indicado en el campo protocolo, o el encabezado del protocolo superior. Los datos consisten de cadenas de octetos y cada octeto puede tener un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama, por lo que el tamaño del campo datos en octetos es:
Tamaño datos=(Longitud total del Datagrama)-(Longitud de la Cabecera).

Por definición el tamaño máximo de un datagrama IP es de 65535 bytes y suponiendo que no se usan opciones la cabecera IP es de 20 bytes por lo que quedan 65514 bytes para datos.
El área de datos será utilizada arbitrariamente por el protocolo TCP o UDP.

Proceso de fragmentación y reensamblado de datagramas IP
Cuando un datagrama IP viaja de un host a otro puede cruzar distintas redes físicas, estos datagramas serán encapsulados en tramas de la capa de enlace de las redes físicas.
Los datagramas IP van a tener un tamaño máximo dependiendo del medio físico de la red que atraviesen, ese tamaño se conoce como la unidad máxima de transmisión MTU (Maximum Transfer Unit). El MTU de una red es la mayor cantidad de datos que puede transportar su trama física. Las redes no pueden transmitir paquetes de longitud mayor a la MTU.
La fragmentación y reensamblado convierten los datagramas IP en el formato requerido por cada una de las redes.
La fragmentación divide los paquetes en varios fragmentos de menor longitud mientras el ensamblado hace lo contrario. Este proceso se hace en los niveles más bajos de modo que los niveles superiores no se percaten de ello.
IP requiere que cada enlace tenga un MTU de al menos 68 bytes de modo que si cualquier red proporciona un valor inferior la fragmentación y el reensamblado tendrán que implementarse en la capa de interfaz de red de forma transparente a IP. El valor de 68 es la suma del mayor valor que puede tener la cabecera IP, de 60 bytes y el tamaño mínimo posible de los datos en un fragmento, 8 bytes.
Las implementaciones de IP no están obligadas a manejar datagramas sin fragmentar mayores a 576 bytes, pero la mayoría podrá manipular valores más grandes, típicamente ligeramente mas de 8192 bytes o mayores y raramente menos de 1500 bytes.
Un datagrama sin fragmentar tiene a cero toda la información de fragmentación como la bandera fc y él fo(fragment offset).
El mecanismo de fragmentación del nivel IP es el siguiente:

1. Se comprueba si el bit indicador de bandera DF permite la fragmentación. Si esta a 1 el datagrama se desecha y se devuelve un error al emisor usando ICMP, sí esta a 0 sé continua con el paso 2.
2. Se comprueba si el campo datos se puede dividir en 2 o más fragmentos basándose en el valor MTU. Todas las nuevas porciones de datos excepto la ultima serán de longitud múltiplo de 8.
3. Las partes en que se ha dividido el campo Datos se colocan en formato de datagramas IP y se tratan como cualquier otro datagrama cuya cabecera será una copia de la cabecera original con las siguientes modificaciones:

- El host asigna el mismo ID a cada fragmento que compone el datagrama.
- El bit de mas fragmentos (MF) sé inicializa a 1 en todos y cada uno de los fragmentos excepto en el ultimo que se pone a cero.
- El campo offset (fo=fragment offset) de cada fragmento sé inicializa al lugar ocupado por cada fragmento de datos en el datagrama original no fragmentado con respecto al comienzo del mismo. Su valor se mide en unidades de 8 bytes.
- Si hay opciones en el datagrama original, el bit de orden superior del byte "type option" determina si se copiaran o no en todos los fragmentos o solo en el primero.

Las opciones de ruteo de la fuente deben copiarse por defecto en todos los fragmentos.
- Sé inicializa el campo de longitud (length) del nuevo datagrama.
- Se inicializa el campo de longitud (length) total del nuevo datagrama.
- Se recalcula el checksum.

4. Cada uno de estos datagramas se envía como un datagrama IP normal independiente, es decir los fragmentos pueden atravesar diversas rutas hacia su destino, y pueden estar sujetos a nuevas fragmentaciones si pasan por redes con MUTs inferiores.

En el host destino se realiza el proceso de reensamblado, el cual independientemente del orden en que le lleguen los fragmentos con el identificador y el offset se pueden reensamblar. Los fragmentos que le van llegando al destino se identifican con el campo ID junto con las direcciones IP fuente y destino del datagrama. También se checa el campo del protocolo.

El receptor destina un buffer de almacenamiento en cuanto llega el primer fragmento. Empieza una rutina con el arranque de un temporizador con el valor del campo TTL de la cabecera IP, el proceso va guardando en buffer los fragmentos que le llegan, cuando se agota el temporizador si no han llegado al destino todos y cada uno de los fragmentos se descarta el datagrama original. Si llegan antes de que expire el temporizador se copian los datos en un buffer en el lugar que indica el campo offset de cada fragmento y se forma de esta manera el datagrama original y continua su procesamiento.

IP no proporciona el contador de reensamblado. Tratará cada datagrama, fragmentado o no de la misma forma. Depende de la capa superior el implementar un timeout y reconocer la perdida de fragmentos. Estas capas podrían ser TCP o UDP.

Funcionamiento de IP en un router.

Cuando un router recibe un paquete, el paquete es pasado a la capa IP que realiza los siguientes pasos:

1) Decrementa el valor TTL al menos en 1. Puede ser disminuido en una cantidad mayor si el router estuviese congestionado. Si alcanza el valor de cero será descartado.
2) El protocolo IP puede fragmentar el paquete en paquetes más pequeños, si el paquete fuese demasiado largo para las líneas de salida del router.
3) Cuando fragmenta el paquete a cada fragmento le agrega una nueva cabecera que incluye:

- Un indicador (flag) de que sigue nuevos fragmentos.
- Un identificador de fragmento para identificar todos los fragmentos que continúan
- Un desplazamiento (offset) para permitir que la maquina que lo va a recibir sea capaz de reensamblar el paquete.

4) IP calcula el checksum.
5) IP obtiene la dirección hardware del siguiente router.
6) Envía el paquete.

En el siguiente host el paquete subirá en el stack de protocolos hasta el TCP o UDP. Este proceso se repite en cada router hasta que el paquete encuentra su destino final. Cuando el paquete llega a su destino final el IP ensamblara las piezas para obtener el paquete original.

Así el ruteador:

- Siempre obtendrá de la cabecera del datagrama IP la dirección de destino.
- A partir de la dirección IP de destino obtendrá la dirección de red de destino.

- Con la dirección de red de destino buscará en su tabla de enrutamiento la mejor ruta.

El datagrama IP es encapsulado en la trama de red subyacente, Fig. 3.3.2.9, que suele tener una longitud máxima, dependiendo del hardware usado. Para Ethernet la longitud será típicamente de 1500 bytes.

Fig. 3.3.2.9 Encapsulado del datagrama IP dentro de la trama de red física.

En vez de limitar el datagrama a un tamaño máximo IP puede tratar la fragmentación y el re-ensamblado de sus datagramas. En particular IP no impone un tamaño máximo pero establece que todas las redes deberían ser capaces de manejar al menos 576 bytes. Los fragmentos de datagramas tienen todos una cabecera copiada básicamente del datagrama original y de los datos que le siguen. Se tratan como datagramas normales mientras son transportados a su destino. Si uno de los fragmentos se pierde todo el datagrama se considerara perdido y los restantes fragmentos se consideraran perdidos.

3.3.3 Direcciones IPv4

El protocolo IP identifica a cada computadora que se encuentra conectada a la red mediante su correspondiente dirección de Internet (IP address).
La dirección IP es un numero que sirve para identificar tanto a un equipo o dispositivo que trabaja con TCP/IP como a la red a la que pertenece dicho equipo, esta dirección debe ser única e irrepetible o de lo contrario provocara conflictos en la red.

Representación de direcciones IP.
La dirección IP es un identificador único dentro del contexto de IP, de 32 bits de longitud divido en 4 campos de 8 bits:
Dirección IP= 4 octetos o bytes= xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
Donde: x=0 o x=1.
Los 32 bits se separan en 4 grupos de 8 bits y cada octeto se representan como si estuvieran separados por un punto, por conveniencia y una mejor comprensión se representa cada octeto en notación punto decimal:
Dirección IP = w.x.y.z = 45.198.119.245
Cada un de los octetos puede tomar un valor desde 0 hasta 255 dependiendo de los bits que estén encendidos en el octeto. Los octetos se representan en formato decimal pero su valor proviene de la conversión del formato binario al decimal:
Octeto = 8 bits = XXXXXXXX
Byte = 00000000 = 0
Byte = 11111111 = 255

- Cada red física tiene su propia y única dirección de red.
- Cada host tiene su propia y única dirección.

Los ruteadores y gateways pueden tener una o más direcciones IP dependiendo del numero de interfaces que posean.

La dirección IP se divide dos partes, una parte de red y un parte de host (dispositivo que posee una dirección IP), Fig. 3.3.3.1.

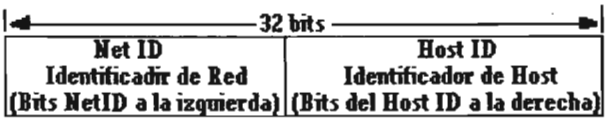


Fig.3.3.3.1 Estructura de la dirección IP

- El Net ID identifica la red a la que pertenece el equipo. Todos los hosts de la misma red física deben tener asignado el mismo NetID para poder comunicarse entre ellos. Los bits que componen al Net ID siempre están a la izquierda.
- El Host ID identifica a un host de otro dentro de una misma red física con su respectivo Net ID. Los bits que componen al Host ID siempre están a la derecha.

Los espacios de direcciones (Net ID) son administrados y asignados por algunos organismos creados exclusivamente para esto:

- El IAB (Internet Activities Board) es el organismo responsable de definir los estándares de facto de la comunidad Internet.
- El NIC (Network Information Center) es el organismo central de Internet que administra y asigna todos los rangos de direcciones que forman el Net ID en una dirección IP y que hacen la dirección única en toda Internet.
- El IANN asigna las direcciones de América y parte de África al ARIN.
- El NIC-México es el organismo al que se le asigna un segmento de direcciones para ser utilizados en la Republica Mexicana.

Clases de direcciones

Para una mejor organización en el reparto de rangos de direcciones las redes se han agrupado en clases, de modo que según el tamaño de la red se optara por un tipo u otro.
La asignación del direccionamiento IPv4 se realiza por rangos para minimizar las tablas de ruteo.
Existen cinco clases de direcciones IP o rangos (A-E), para identificar que clase de dirección se tiene se debe observar el primer octeto de izquierda a derecha ya que las clases son identificadas a partir de los tres primeros bits de orden mas alto. Cada clase contiene a un rango de direcciones establecido:

Direcciones clase A

Este tipo de direcciones es usado para redes muy grandes (redes que tienen mas de 2^{16} hosts), solo algunas cuantas organizaciones comerciales obtiene una dirección clase A. Lo normal es que se utilicen una o varias redes clase B.
Las direcciones clase A empiezan con 0 (prefijo) por lo que utilizan únicamente 7 bits del primer byte para identificar la red (Net ID). Usa los restantes 24 bits (tres bytes) disponibles para cada uno de los hosts (Host ID) que pertenezcan a esta misma red.
Con esta clase de direcciones solo pueden haber 2^7-2=126 redes cada una con 2^{24}-2= 16, 777,214 hosts.
El rango en decimal es desde la IP 1.0.0.0 hasta la 126.0.0.0
Por lo tanto hay dos formas de distinguir una red clase A:

- Estando en formato binario si el primer octeto de izquierda a derecha empieza con 0 es una red clase A
- Estando en formato decimal punteado si el primer byte tiene un valor comprendido entre 1 y 126 e s una red clase A.

Direcciones clase B

Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes que tengan redes de tamaño medio, de hasta 2^{16} hosts. En caso de que el número de ordenadores que se necesitara fuera mayor seria posible obtener mas de una dirección de clase B, para evitar el uso de una clase A.

En esta clase de direcciones el identificador de red (NetID) se compone de los dos primeros bytes de la dirección, además que los dos primeros bits (prefijo) de una red clase B siempre son 1 y 0 por lo que usan 14 bits para la parte de NET ID, estos dos octetos pueden tener un valor entre 128.1 y 191.254 (128.0 y 191.255 no se pueden usar por ser de significado especial). Los dos últimos bytes (16 bits) de la dirección constituyen el identificador de host (Host ID).

Esta clase de direcciones permite tener 2^{14}-2=16,382 redes con 2^{16}-2= 65,534 hosts en cada red.

El rango de direcciones es de la 128.0.0.0 hasta la 191.255.0.0 o 128.1.0.0-191.254.0.0

Las dos formas de distinguir una red clase B son:

- Estando en formato binario si el primer octeto de izquierda a derecha empieza con 10 es una red clase B.
- Estando en formato decimal punteado si el primer byte tiene un valor comprendido entre 128 y 191 e s una red clase B

Direcciones clase C

Esta clase permite tener un gran numero de redes con pocos hosts, permite tener redes con menos de 2^8 hosts. El prefijo de estas redes siempre es 110.

Las direcciones clase C usan los tres primeros bytes (21 bits) para el numero de red y tienen solo 8 bits para la parte de los hosts que pertenecen a cada red.

Estas redes empiezan siempre con 110, permiten tener cerca de 2^{21}-2=2,097,150 redes con 2^8-2= 254 hosts cada una.

El rango de direcciones clase c es desde la 192.0.1.0 hasta la 223.255.255.0 o 192.0.1.0-223.255.254.0

Una red clase B se identifica de las siguientes dos formas:

- Estando en formato binario si el primer octeto de izquierda a derecha empieza con 110 es una red clase C.
- Estando en formato decimal punteado si el primer byte tiene un valor comprendido entre 192 y 223 es una red clase C.

Las direcciones de clase A a la C se conocen como direcciones homologadas o publicas, Los números dados de redes que se pueden tener y hosts se nombran en función de los bits que se utilizan para identificar cualquiera de las dos partes de una red, pero en realidad esas cantidades de hosts y redes no son las cantidades exactas, en la realidad son menores ya que dentro de cada clase hay algunas direcciones especiales que se usan para propósitos especiales como son las redes privadas, de loopback de broadcast, etc.

Direcciones clase D

Las direcciones clase D se usan para definir grupos de hosts por multicast (multidestino) en un área limitada, para cuando se quiere transmitir información a esos grupos de maquinas. Son usadas por los ruteadores y protocolos de ruteo.
Los cuatro primeros bits del prefijo siempre son 1110.
El rango de direcciones clase D va desde 224.0.0.0 hasta la 239.255.255.255
Multicast
El multicast elimina el sobreencabezado causado por la falta de selectividad del broadcasting al usar grupos de direcciones IP. Cada grupo esta representado en un numero de 28 bits mas los cuatro bits de inicio 1110 incluidos en una dirección de clase D. De este modo se tienen las direcciones de grupo de multicast desde 224.0.0.0 a 239.255.255.255. Para cada dirección de multicast hay un conjunto de cero o más hosts que escuchan. Para que un host envíe un mensaje a ese grupo no se requiere que pertenezca a ese grupo. Hay dos clases de grupos de hosts:

- Permanentes

La dirección IP tiene una asignación permanente a través del IANA. Un host puede unirse a un grupo o dejarlo a su voluntad. Algunos de los grupos importantes asignados son:

Dirección Multicast	Asignación
224.0.0.0	Dirección base reservada
224.0.0.1	Todos los sistemas en esta subred
224.0.0.2	Todos los routers en esta subred
224.0.0.5	Todos los routers OSPF
224.0.0.6	Routers OSPF designados

- Provisionales

  Cualquier grupo que no sea permanente es provisional y esta disponible para ser asignado dinámicamente según las necesidades. Los grupos provisionales dejan de existir cuando el numero de sus miembros se hace cero.

Direcciones clase E

Direcciones para investigación y/o uso futuro.
Siempre empiezan con el prefijo 11110.
El rango va desde 240.0.0.0 hasta la 247.255.255.255

La mayor ventaja de la codificación de información de red en las direcciones de red IP es que es posible realizar un ruteo. También se tiene la ventaja de que las direcciones de red IP se pueden referir tanto a redes como hosts. Por regla nunca se asigna un campo host ID igual a 0 a un anfitrión individual. En vez de eso una dirección IP con campo host ID igual a 0 se utiliza para referirse a la red en sí misma.
Otra ventaja significativa del esquema de direccionamiento IP es que incluye una dirección de difusión (Broadcast) que se refiere a todos los hosts de la red. De acuerdo con el estándar cualquier campo host ID consistente solamente de 1´s esta reservado para la difusión. Esto permite que un sistema remoto envíe un solo paquete que será difundido en toda la red especificada. Así para implementar estas y otras ventajas del direccionamiento IP se tienen las siguientes direcciones especiales.

Direcciones especiales

Las direcciones especiales son casos especiales entre las clases A, B y C por lo que no se deberían usar ya que están reservadas:

- Las direcciones en el rango 0.0.0.0-0.255.255.255 y 128.0.0.0.
  Se usan para identificar a la red de cualquier host, o host propio. Toda la parte de Host ID (Direcciones IP con Host ID=0) en ceros significa "esta red". Toda la parte de Net ID (Direcciones IP con Net ID=0) en ceros significa "este host". Este tipo de direcciones se reserva para las maquinas que no conocen su dirección, pudiendo usarse para solicitar tanto la identificación de red para maquinas que aun no conocen el numero de red a la que se encuentran conectadas, como la identificación de host para maquinas que aun no conocen su numero de host de la red o en ambos casos, esta solicitud se hace a un servidor remoto. Permitido solamente en el arranque del sistema, pero nunca es una dirección de destino valida. La dirección 0.0.0.0 se conoce como encaminamiento por defecto y tiene que ver con el camino por el que el protocolo IP encamina los datagramas.
- Las direcciones en el rango de 255.0.0.0 a 255.255.255.255
  Son direcciones de broadcast general en Internet, o de anuncio de direcciones (broadcast addresses), estas direcciones hacen referencia a todos los hosts de la misma red o a todas las redes. Cualquier dirección local (Dirección IP con Host ID=1) compuesta de puros 1s esta reservada para broadcast y una dirección que contenga sus 32 bits en 1 (Dirección IP con Net ID=Host ID=1) se considera un mensaje difundido a todas las redes y a todos los dispositivos. Puede ser útil cuando se necesita enviar el mismo datagrama a un numero determinado de hosts en la misma red resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. También se puede usar cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente numero IP y no se conoce la dirección del servidor de nombres de dominio más cercano. Lo usual cuando se quiere hacer broadcast es que se utilice una dirección compuesta por el identificador normal de la red y por el numero 255 (todos unos) de cada byte que identifique al host. Por conveniencia también se permite el uso del numero 255.255.255.255 con la misma finalidad de forma que resulte más simple referirse a todos los sistemas de la red. Normalmente los routers no deben dejar pasar las direcciones de broadcast. Las direcciones de broadcast nunca son validas como direcciones fuente, solo como direcciones destino.

Los diferentes tipos de broadcast son:

- Direcciones de broadcast limitado.
  La dirección 255.255.255.255 se usa en redes que soportan broadcast y se refiere a todos los hosts de la subred <red><host=111...1>. No requiere que el host tenga conocimiento de la configuración IP. Todos los hosts de la red local reconocerán la dirección, pero los routers nunca enviaran el mensaje. El protocolo BOOTP emplea el broadcast limitado para permitir a estaciones de trabajo sin disco contactar con un servidor BOOTP.
- Direcciones de broadcast dirigidas a red.
  Este tipo de broadcast se realiza si el numero de red es uno valido, la red no se subdivide en subredes y el host tiene todos sus bits a 1. Este tipo de broadcast se utiliza en solicitudes ARP en redes que contienen subredes.
- Direcciones de broadcast dirigidas a subred.

Si él número de red y el de subred son válidos y el de host tiene todos sus bits a 1, entonces la dirección hace referencia a todos los hosts de la subred especificada. El broadcast lo efectúa realmente el router de la subred que recibe el datagrama.

- Direcciones de broadcast dirigidas a todas las subredes.

Este tipo se realiza si un numero de red es valido, la red se subdivide en subredes y la parte local de la dirección tiene todos los bits a 1 y la dirección se refiere a todos los hosts en todas las subredes de la red especificada

- Las direcciones del rango desde 127.0.0.1 hasta la 127.255.255.254 son direcciones de loopback. Estas direcciones son tomadas por el equipo como direcciones realimentadas. Cualquier paquete que se mande a una dirección IP de este rango en realidad no sale del equipo transmisor ya que lo que sale del controlador de salida se encamina directamente al controlador de entrada sin pasar a la red.
- Las direcciones 191.255.X.X y 223.255.255.X se usan para enmascarar.
- Las direcciones 192.168.X.X están reservadas para las intranets.

Direcciones privadas

Dentro de las clases A-C existe un grupo de direcciones especiales que reservan parte del espacio de direcciones para redes privadas se usan exclusivamente dentro de una organización que no requiere conectividad IP con Internet. Por lo tanto se recomienda que se use un grupo de esta clase de direcciones para configurar en nuestra red. Estas direcciones son conocidas como direcciones no homologadas o privadas. Estas direcciones no son ruteables en Internet por lo que sí son usadas en una red LAN para salir a Internet se necesita al menos una dirección homologada. Hay tres rangos de direcciones que IANA ha reservado para este propósito:

- Una sola red de clase A: 10.0.0.0-10.255.255.255.
- De la clase B reserva 16 redes contiguas:172.16.0.0-172.31.255.255
- De la clase C 256 redes contiguas: 192.168.0.0-192.168.255.255.

Cualquier organización puede usar cualquier dirección en estos rangos si no hace referencia a ninguna otra organización. Estas direcciones no pueden ser direccionadas por hosts de otras organizaciones y no están definidas para los routers externos. Se supone que los routers de una red que no usa redes privadas, particularmente aquellos operados por proveedores de servicios de Internet, han de desechar toda información de encaminamiento relativa a estas direcciones. Los routers de una organización que utiliza direcciones privadas deberían limitar todas las referencias a direcciones privadas a los enlaces internos, no deberían hacer publicas las rutas a direcciones privadas ni enviar datagramas IP con estas direcciones a los routers externos. Los hosts que solo tienen una dirección IP privada carecen de conexión IP con Internet.

En la Fig. 3.3.3.2 tenemos las clases de direcciones.

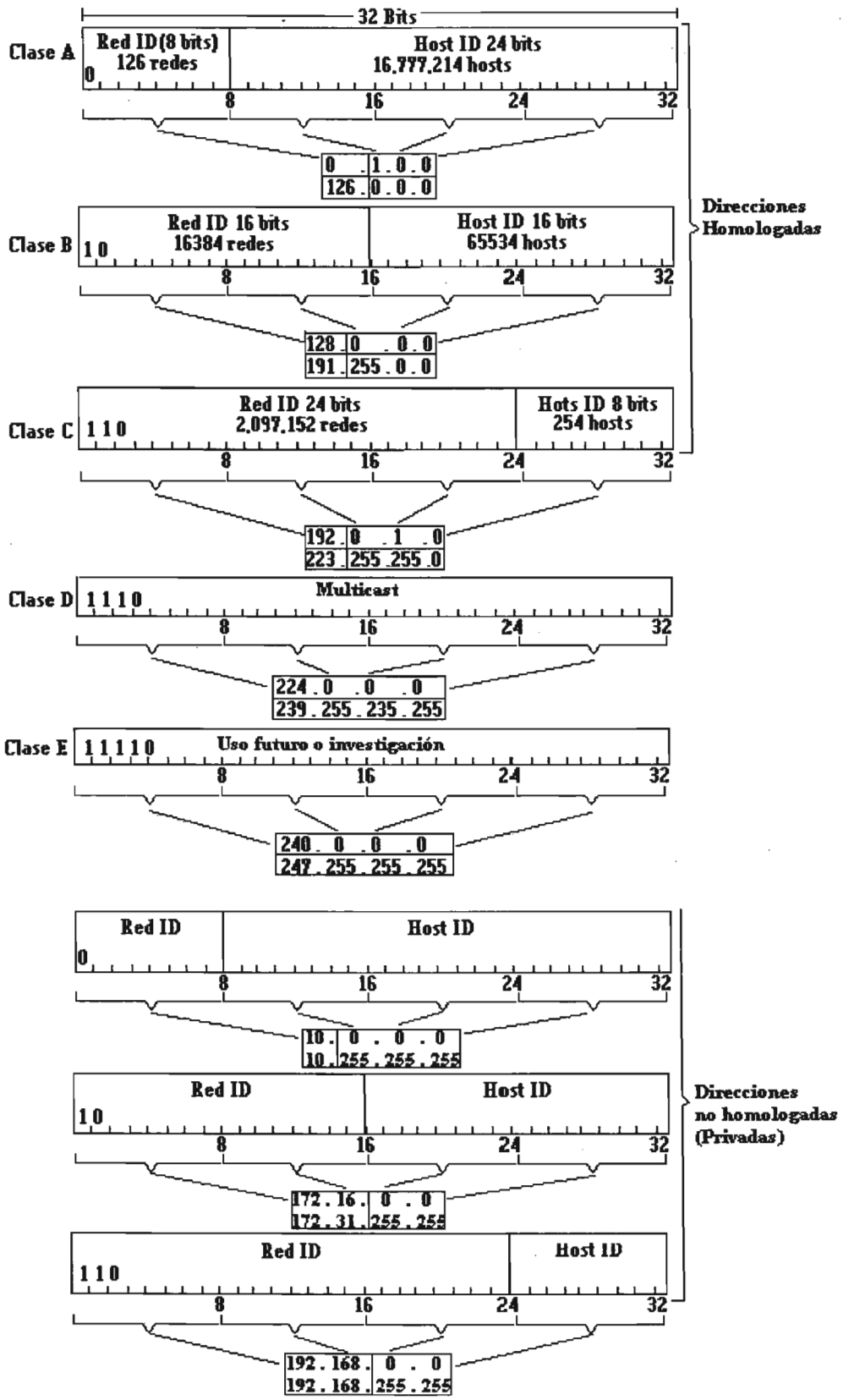


Fig. 3.3.3.2 Formatos de las clases de direcciones IP

En la tabla 3.3.3.1 tenemos los rangos de direcciones de red

Clase	Inicio del rango	Fin del rango
Clase A	0.1.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.1.0	223.255.255.0
Clase D	224.0.0.0	239.255.235.255
Clase E	240.0.0.0	247.255.255.255
Privadas	10.0.0.0	10.255.255.255
Privadas	172.16.0.0	172.31.255.255
Privadas	192.168.0.0	192.168.255.255
Loopback	127.0.0.1	127.255.255.254
Cualquier host	0.0.0.0	0.255.255.255
Broadcast General	255.0.0.0	255.255.255.255

Tabla 3.3.3.1 Rangos de direcciones IP

Las direcciones de red son las que definen el enrutamiento en Internet, ya que los equipos encargados de realizar el ruteo o encaminamiento de los paquetes procesan la parte de red de las direcciones IP. Las direcciones de red se forman poniendo en 0 toda la parte de host, así para las clases A, B, y C tendríamos en forma general su dirección de red:
Clase A w.0.0.0
Clase B w.x.0.0
Clase C w.x.y.0

De las clases de direcciones A, B y C los rangos de hosts que tenemos disponibles son mostrados en la tabla 3.3.3.2

Clase	Inicio del rango	Fin del rango
Clase A	w.0.0.1	w.255.255.254
Clase B	w.x.0.1	w.x.255.255
Clase C	w.x.y.1	w.x.y.254

Tabla 3.3.3.2 Rangos de hosts por clase de dirección

La desventaja de este esquema de direcciones es que si cambia un computador de una red a otra, su dirección IP debe cambiarse tambien. Y si varia el tamaño de una red es posible que también varíe la clase de direcciones.

El agotamiento de las direcciones IP
El numero de redes en Internet estuvo duplicándose durante varios años, siendo las redes clase B las de mayor uso y con una tendencia a agotarse desde el año 1994, mientras las redes clase C apenas si se usaban. La razón de esto era la facilidad de las redes clase B para permitir a las organizaciones crecer a futuro, la gran mayoría de estas redes clase B estaban asignadas a redes pequeñas.
Debido a esto la política del InterNIC sobre la concesión de números de red cambia desde 1990 para preservar el espacio de direcciones existente, en particular para frenar el agotamiento de direcciones de clase B. Las nuevas políticas son:

- La mitad superior del espacio de direcciones de clase A se reserva indefinidamente para su uso en la transición a un nuevo sistema de numeración.
- Las redes clase B solo se asignan a organizaciones que comprueban su necesidad de uso al igual que con las de clase A. Cualquier solicitud de clase A se analiza estrictamente el caso particular. Los requerimientos para las redes de clase B son que la organización solicitante
    - Tenga un esquema de subnetting con mas de 32 subredes dentro de su red operativa.
    - Tenga mas de 4096 hosts.
- A las organizaciones que no satisfacen los requerimientos para una red clase B se les asigna un bloque de redes de clase C numeradas consecutivamente.
- La mitad inferior del espacio de direcciones de clase C (números de red del 192.0.0 al 223.25.245) se divide en 8 bloques para las autoridades regionales que están reservadas del siguiente modo, tabla 3.3.3.3:

Región	Bloque de dirección
Multiregional	192.0.0-193.255.255
Europa	194.0.0 – 195.255.255
Otros	196.0.0 – 197.255.255
Norteamérica	198.0.0 – 199.255.255
Centro y Sudamérica	200.0.0 – 201.255.255
Borde del pacifico	202.0.0 – 203.255.255
Otros	204.0.0 – 205.255.255
Otros	206.0.0 – 207.255.255

Tabla 3.3.3.3 Bloques de direcciones reservados para las autoridades regionales.

El rango multiregional incluye las redes de clase C que habían sido asignadas antes de que se adoptara este nuevo esquema. Los rangos definidos como otros se utilizan donde hace falta flexibilidad por encima de las limitaciones de las fronteras regionales.
La mitad superior del espacio de direcciones clase C (208.0.0 a 223.255.255) permanece sin asignar y sin reservar.
Las organizaciones que tienen una serie de números de clase C, el rango asignado contiene números de red contiguos a nivel de bit y el numero de redes de ese rango es una potencia de dos. Es decir todas las direcciones IP en ese rango tienen un prefijo común y cada dirección con ese prefijo esta a su vez dentro del rango. El numero máximo de números de red asignados contiguamente es 64 correspondiente a un prefijo de 18 bits.
Usar números de clase C de esta forma ha frenado el problema del agotamiento de las direcciones de clase B pero no es una solución definitiva a las limitaciones de espacio inherentes a IP.

3.3.4 Redes y Subredes

Mascaras de subred

Para la distinción de redes y subredes es importante definir un concepto importante, la mascara de subred (subnet mask).

La mascara de red es un numero con el formato de una dirección IP de 32 bits expresada en notación decimal que nos sirve para distinguir cuando una maquina determinada pertenece a una subred dada. La mascara nos sirven para definir que bits de la dirección IP representan a la red y cuales al host.

En formato binario todas las mascaras de red tienen los 1´s agrupados a la izquierda y los 0´s a la derecha.

La mascara de subred es un parámetro que indica si la red esta segmentada y determina en cuantas porciones esta dividida.

Cualquier host en una red TCP/IP requiere una mascara de subred, incluso las redes basadas en clases, para reconocerse si están en la misma red física. Las redes con direccionamiento IP que usan identificadores de red basados en clases son redes con un segmento único es decir no están divididas en redes más pequeñas o subredes.

Las mascaras se forman poniendo todos los bits que correspondan a la parte de red (Net ID) a 1 y todos los bits que corresponden a la parte de host (Host ID) a 0. De esta forma la mascara de subred permite distinguir el Host ID del Net ID y es un parámetro que determina si el host es local a la red o es un host remoto que se encuentra en otra red.

La mascara de red divide la dirección IP en:

- Parte de red o prefijo. Los equipos que pertenecen al mismo rango comparten el prefijo.
- Parte de host o de interfaz.

La longitud del prefijo lo indica la mascara de red ya que en los bits correspondientes al prefijo la mascara tiene los bits en 1 y en los correspondientes a la parte de host los bits son 0.

En las redes basadas en clases tenemos las mascaras por omisión o por default. Esta mascara dependerá del tipo de clase de dirección. De esta forma para las direcciones de clase A los bits del primer octeto se ponen a 1 y los bits de los 3 octetos restantes se ponen a 0, al convertir a decimal el resultado es la mascara 255.0.0.0, como los bits de la mascara nos indican entre otras cosas cuantos bits forman al Net ID estas se pueden representar de forma abreviada uniéndolas a la dirección IP con una diagonal, así para la clase A su representación abreviada es /8. Para la clase B tenemos 255.255.0.0 o /16 y para la clase C tenemos 255.255.255.0 o /24. En la tabla 3.3.4.1 tenemos estas mascaras.

Clases De redes	Bits utilizados para las subredes	Notación en punto Decimal	Notación Abreviada
Clase A	11111111 00000000 00000000 00000000	255.0.0.0	/8
Clase B	11111111 11111111 00000000 00000000	255.255.0.0	/16
Clase C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Tabla 3.3.4.1 Mascaras de subred por omisión

Una mascara de subred por omisión en TCP/IP no esta dividida en subredes.

Es importante notar que una mascara de subred aunque tiene el mismo formato decimal y representación técnica no es una dirección IP. La mascara de subred es un numero de 32 bits que se configura junto con la dirección IP de 32 bits también. La mascara tiene 1´s binarios en todos los bits que especifica los campos de red y subred y 0´s binarios en todos los bits que especifican el campo de host.
Con la mascara de red podemos averiguar si dos maquinas están dentro de la misma subred, ya que el proceso interno TCP/IP utiliza los dos números, la dirección IP y la mascara de subred para realizar una operación AND lógica (si ambos bits son 1 el resultado será 1, cualquier otra combinación de bits será 0) entre los bits de la mascara y los bits de la dirección IP. Esta operación aplicada a una sola dirección IP y su correspondiente mascara no indicara cual es el Net ID de la dirección IP, es decir nos muestra cual es el numero de subred. Cuando se aplica a dos direcciones IP con sus respectivas mascaras podemos determinar si esas dos direcciones pertenecen a la misma red física cuando el resultado obtenido nos indique el mismo Net ID de lo contrario una es local a la dirección física y la otra es remota.
Por otro lado podemos tener redes segmentadas debido a que se crean subredes o superredes (subnetting o supernetting) a partir de las redes basadas en clases. En este caso se tendrán mascaras de subred personalizadas, por lo que la mascara de subred indica que la red esta dividida.

Subredes.
Las clases de direcciones de Internet definen tres diferentes escalas de redes IP, los 32 bits de la dirección IP son repartidos entre identificadores de red e identificadores de host dependiendo de cuantas redes y hosts por red son necesarios. En el caso de las redes de clase A que tiene la posibilidad de tener 16 millones de hosts en la misma red, toda esta cantidad de host comparte el mismo dominio de broadcast lo cual saturaría la red por el exceso de trafico, aunando a esto una gran cantidad de direcciones son desperdiciadas ya que no son asignadas con lo que una gran cantidad de direcciones está sin poderse usar en Internet aunque no estén asignadas.
En un esfuerzo para crear dominios de broadcast más pequeños y utilizar mejor los bits del Net ID una red IP se puede dividir en redes más pequeñas o subredes, al proceso de segmentar una red en subredes se le conoce como subnetting donde cada subred es limitada por un ruteador IP y se le asigna un nuevo identificador de subred, el nuevo identificador de subred es un subconjunto del identificador de red basado en clases originales. La subred tiene existencia dentro de la red original pero no respecto al mundo exterior, que sigue viendo una red única.
El direccionamiento por medio de subredes surge como consecuencia del enorme crecimiento de Internet por lo que el numero de hosts que estaban conectados a una red llegaba a ser muy grande y había que realizar una división de la red en dos redes o más de menor tamaño.
Para evitar tener que solicitar direcciones IP adicionales se introdujo el concepto de subred.
Las subredes son redes físicas independientes que comparten un Net ID que identifica a la red principal, la comunicación entre estas se logra por medio de la mascara de subred.
De lo anterior tenemos que una subred se define como un dominio de administración.
Las subredes tienen como objetivo abatir el tráfico de red ya que segmentar o particionar la red lógica en un numero optimo de subredes de menor tamaño aumenta el desempeño de la rapidez de búsqueda y de acceso a los recursos de red.

Algunas razones que justifican el uso de subredes son:

- Reducir la congestión de red.
- Mezclar diversos componentes de la red o de las tecnologías.
- Descentralizar y facilitar la administración del direccionamiento IP.
- Razones geográficas.
- Minimizar el número de direcciones de red en uso ya que múltiples redes físicas pueden compartir el mismo prefijo de red IP.
- El tener un gran número de redes triviales resulta en:
  - Tablas de ruteo extremadamente grandes.
  - Abuso del espacio de direcciones limitado.
- Alcanzar las metas de:
  - Minimizar el tamaño de las tablas de ruteo.
  - Maximizar el uso de una dirección de red dada.

Localmente cada subred actúa como una red diversa e independiente, por lo que la comunicación entre ordenadores en diversas subredes no será posible a menos que los medios se proporcionen para lograr esto.
Las subredes se crean a partir de las redes basadas en clases, en las cuales se toma prestado un numero adecuado de bits de los octetos que forman la parte de Host ID para formar las subredes necesarias, esos bits prestados forman el campo de subred, así por ejemplo si se tiene una red clase B y se toman los 8 bits del primer octeto que forma la parte de Host ID tendremos ahora la posibilidad de tener 254 subredes con 254 hosts cada una. Así en lugar de tener una sola red con 65,534 hosts pasaremos a tener 254 subredes con únicamente 254 hosts en cada subred, como se puede ver el trafico en cada una de estas subredes es mucho menor a l de la red clase B. Los 8 bits tomados para segmentar la red, serán usados para formar el nuevo identificador de subred.
Lo importante de las subredes es que no es necesario reconfigurar el resto de la red IP. Ya que las subredes son consideradas por el resto de la red como parte de red IP original o basadas en clases.
Las subredes se conocen también con el nombre de redes classless debido a que no pertenecen a las clases de direcciones puras (A, B, C, D, E).
En una subred el numero de host de la dirección IP se subdivide en un numero de subred y uno de host. Esta segunda red se denomina subred. La red principal consiste ahora en un conjunto de subredes. Ahora la dirección IP se interpreta como:
< Numero de red><Numero de subred><Numero de host>
La combinación del numero de subred y del host suele denominarse dirección local o parte local. La creación de subredes se implementa de forma que sea transparente a las redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de una red distinta sigue considerando la parte local de la dirección IP como un numero de host.
La división de la parte local de la dirección IP en números de subred y de host es de libre elección del administrador local, cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando la mascara de subred. Los bits a cero en la mascara de subred indican las posiciones de bits correspondientes al numero de host y los que están en uno posiciones de bits correspondientes al numero de subred. Las posiciones de la mascara pertenecientes al numero de red se ponen a uno pero no se usan.

Para la asignación de los bits que compondrán la subred lo normal es usar un bloque de bits contiguos al comienzo de la parte local para el numero de subred ya que así las direcciones son más legibles. Con este enfoque cualquier mascara de subred con bits 1 contiguos es valida pero una con bits discontinuos no es valida:
255.255.255.252=11111111 11111111 11111111 11111100 Subred con únicamente 1 host
255.255.255.15=11111111 11111111 11111111 00001111 Bits 1 discontinuos

Tipos de subnetting
Existen dos tipos de subnetting (subredes): el estático y el de longitud variable. El de longitud variable es el más flexible de los dos. El tipo de subnetting disponible depende del protocolo de encaminamiento en uso, el IP nativo solo soporta subnetting estático al igual que el protocolo de ruteo ampliamente utilizado RIP. La versión 2 del protocolo de ruteo RIP ya soporta subnetting de longitud variable.

Subnetting estático
El subnetting estático consiste en que todas las subredes de la red dividida empleen la misma mascara de subred. Este tipo de subnetting implica el desperdicio de direcciones en redes pequeñas. Por ejemplo una red de cuatro hosts que use una mascara de subred de 255.255.255.0 desperdicia 250 direcciones IP, además hace más difícil reorganizar la red con una mascara nueva. Casi todos los hosts y routers soportan subnetting estático.

Subnetting de longitud variable.
Cuando se usa subnetting de longitud variable, las subredes que constituyen la red pueden hacer uso de diferentes mascaras de subred. Una subred pequeña con solo unos pocos hosts necesita una mascara que permita acomodar solo a esos hosts. Una subred con muchos hosts puede requerir una mascara distinta para direccionar esa elevada cantidad de hosts. La posibilidad de asignar mascaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de red. Además una subred se puede dividir en dos añadiendo un bit a la mascara. El resto de las subredes no se verán afectadas por el cambio. No todos los hosts y routers soportan subnetting de longitud variable. Solo se dispondrán redes del tamaño requerido y los problemas de encaminamiento se resolverán aislando las redes que soporten subnetting de longitud variable. Un host que no soporte este tipo de subnetting, deberá disponer de una ruta de encaminamiento a un router que si lo haga.
Siempre que los routers entre las subredes que tengan distintas mascaras usen subnetting de longitud variable, los protocolos de encaminamiento deben ser capaces de ocultar la diferencia entre mascaras de subred a cada host de una subred. Los hosts pueden seguir usando encaminamiento IP básico y desatenderse de las complejidades del subnetting que quedan a cargo de los routers.

Determinación del numero de red mediante la mascaras de subred
Los routers ejecutan un conjunto de procesos para determinar la red (y para subnetting la subred). Primero el router extrae la dirección IP destino del paquete de entrada y recupera la mascara de subred interna. Ejecuta una operación lógica AND para obtener el numero de red. Esto causa que la porción de host de la dirección destino IP sea removida mientras el numero de red destino permanece. El router observa el numero de red destino y lo hace

corresponder con una interfase de salida. Finalmente retransmite el paquete a la dirección IP destino.
El por que algunos hosts no soporten subnetting esta en el algoritmo que realiza el encaminamiento IP, en hosts que no soportan subnetting el algoritmo únicamente compara la parte de la dirección de red destino con la suya si son iguales manda el datagrama a la red local o al gateway que le correponde a la dirección. Con subnetting el algoritmo tiene que realizar la operaciones AND de la dirección IP destino y su mascara así como con la dirección local que recibe el datagrama y su mascara, si el resultado de las operaciones AND es el mismo transmite el datagrama a la red local, de lo contrario la manda al gateway correspondiente. Como se puede ver el procedimiento que tiene que realizar el protocolo de encaminamiento es diferente con subnetting que sin ella.
Los puntos importantes para subnetear una red son:

- Temer una red o determinar la clase de dirección que se usara para segmentar.
- Determinar el numero de subredes requeridas:
  - Uno por cada subred.
  - Uno por cada conexión WAN.
- Determinar el numero de hosts por subred:
  - Uno por cada host de TCP/IP.
  - Uno por cada interfaz de router.
- Definir una mascara de subred apropiada para la segmentación.
- Definir un único Subred ID para cada segmento físico y en base a la mascara de subred.
- Definir el rango de hosts validos para cada subred en base al subred ID.

Numero de subredes
El numero de subredes y hosts se determinaran en base a las necesidades que se tengan de áreas, regiones o puntos, interfaces a interconectar a las subredes y de acuerdo a las necesidades en el futuro por lo que el numero de subredes debería ser el doble o cuando menos un 10% mayor al necesario actualmente. En este punto es importante tener en cuenta para efectos de diseño que entre mas subredes menos hosts y viceversa.

Definición de la mascara de subred
Una subred se define mediante la aplicación de una mascara (un conjunto de bits activados o desactivados) a la dirección IP. Si el bit de la mascara esta activo (valor 1) el correspondiente bit se interpreta como un bit de dirección de subred, mientras que si un bit de la mascara esta desactivado (valor 0) dicho bits era interpretado como un bit de dirección de host. Es decir para calcular la dirección de red pondremos a cero todos aquellos bits que estén a cero en la mascara y dejaremos el resto sin alterar, mientras que para calcular la dirección de host pondremos a cero los bits que coincidan con los unos de la mascara y dejaremos el resto sin alterar.
Para definir la mascara de subred tenemos los siguientes pasos:

1. Una vez determinado el numero de segmentos físicos de la red o números de subredes, se calcula cuantos bits en sus combinaciones cubren el numero de subredes necesitado para ello aplicamos la siguiente formula:

$2^n-2 \geq$ Num. de subredes

Donde n es el numero de bits que se tomaran de la parte de Host ID para subnetear.

2. El numero de n bits necesarios para subnetear se sustituyen en la mascara original en el valor más significativo de la porción de Host ID.

Ahora las mascaras de subred tendrán tres partes: Net ID, Subnet ID y Host ID como muestra la Fig. 3.3.4.1

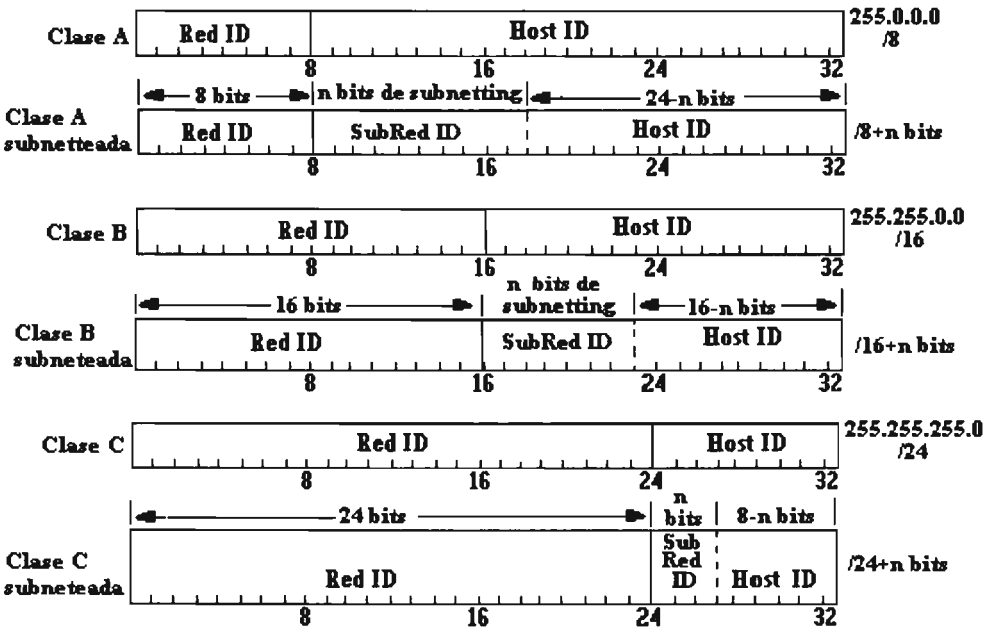


Fig. 3.3.4.1 Mascaras de subred

3. Se convierte a decimal el nuevo valor binario lo que nos proporciona la mascara de subred.

Definición de los IDs de las subredes.

Para definir los ID de las subredes se siguen los siguientes pasos:

1. Poniendo a cero los bits que pertenecen a la parte de Host ID, con el numero de bits que se van a usar, para subnetear se listan sus posibles combinaciones.
2. Se descartan las combinaciones igual a cero y uno de los bits de subneteo.
3. Se convierten a decimal los ID de la subred para cada subred. Cada valor será un rango de ID de subredes valida para los hosts de cada subred.

Este método se puede usar si el numero de bits para subnetear es pequeño pero cuando el numero de bits es de mas de 3 listar todas las combinaciones es un proceso largo, por lo que se puede usar el siguiente método:

1. Listar el numero de bits usados para subnetear en orden ascendente.
2. Convertir el bit mas bajo a decimal, este será el valor de incremento para cada subred.
3. Iniciando desde cero los valores para cada combinación de bits hasta llegar al valor máximo definido por todos los bits usados para subnetear del paso 1.

Definición de los rangos de host validos
Para definir el rango de hosts nos basamos en cada ID de subred. Cada ID indicara el valor inicial del rango mas 1, el valor final del rango será menor que el valor de inicio del siguiente rango de subred.

Supernnetting
La gran diversidad de cambios en el ambiente del direccionamiento IP, provoca que diversas técnicas de direccionamiento alterno a las subredes sean establecidas. En este aspecto se han desarrollado tres técnicas para implementar las superredes:

- VLSM.
- Summarizing.
- CIDR.

El surgimiento de estas técnicas fue debido a que el gran crecimiento de la demanda de Internet provoca que se tenga que establecer algún método de agrupación de los millones de registros IP que recibe un dispositivo de ruteo o switcheo. Algunos temas de literatura de internetworking consideran a las tres técnicas ramas de las superredes mientras alguna otra literatura solo considera al CIDR como supernetting real.

- VLSM

Esta técnica se conoce como subneteo de longitud variable VLSM (Variable Length Subnet Mask) consiste en subdividir nuevamente un dominio de subred. Esto es, cuando se tiene una red subneteada se le puede volver a aplicar otro subneteo. El procedimiento para realizar esto es exactamente el mismo que se usa para subnetear una red.
Cuando se usa VLSM, las subredes que forman la red pueden usar diferentes mascaras de subred. De esta forma una subred pequeña con solo unos pocos hosts necesita una mascara que permita acomodar solo esos hosts. Por otro lado una subred con muchos hosts puede requerir una mascara distinta para direccionar la mayor cantidad de hosts. El poder asignar mascaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de red. Una subred se puede subdividir en dos añadiendo un bit a la mascara y el resto de las subredes no se verán afectados por el cambio. No todos los hosts y ruteadores soportan subnetting de longitud variable.

- Summarizing

La sumarización es realizada por los ruteadores con protocolo classful durante la convergencia de ruteadores.
La sumarización agrupa diferentes redes clase A y B en una sola red, así como redes clase C. La operación que se realiza agrupa direcciones de red de acuerdo a un prefijo común a nivel binario y a este mismo nivel los bits considerados de orden común serán los que definan en igual cantidad de numero a la mascara de red.
Para esto si se tiene varias redes clase B con algunos bits comunes estos se usan para agruparlos en una sola red con la mascara incluyendo esos bits comunes, por ejemplo si se tienen 4 redes clase B 130.120.2.0/23, 130.120.12.0/23, 130.120.18.0/23, 130.120.24.0/23, estas 4 redes tienen los tres primeros bits del tercer octeto común.
130.120. 2.0=130.120.000 00010.0
130.120.12.0=130.120.000 01100.0
130.120.18.0=130.120.000 10010.0
130.120.24.0=130.120.000 11000.0

Por lo tanto se pueden agrupar como una sola red de la forma 130.120.0.0/19, esto es, ahora la subnet mask es de 19 bits o 255.255.224.0

CIDR

Usar rangos de direcciones de clase C en vez de una sola de clase B provoca que cada red tenga que ser direccionada por separado. El encaminamiento IP estándar comprende las clases A, B y C, en cada una de ellas se puede realizar subnetting para tener una mejor granularidad del espacio de direcciones en cada red, pero no hay forma de especificar que existe una relación real entre múltiples redes de clase C. Esto ha provocado el problema de la explosión de la tabla de ruteo, ya que por ejemplo una red clase B con 3000 hosts requiere una sola entrada en la tabla de encaminamiento para cada router troncal, pero si la misma red se direcciona con un rango de redes clase C necesitara 16 entradas.

Uno de los mayores problemas que tiene Internet en la actualidad es la escalabilidad del espacio de direcciones para las redes, dado el gran crecimiento que esta experimentando. Es particularmente ineficiente la clasificación de las direcciones en los tipos A, B, C, D.

Una solución que se ha planteado a estos problemas es incrementar el espacio de direcciones con el procedimiento conocido como CIDR (Encaminamiento en dominio Internet sin clase).

La rigidez del esquema original de clases llevaba a una subutilización de las direcciones por lo que se adopto la modalidad del prefijo de longitud variable.

Este es el único método de supernetting establecido como norma de jure, es el CIDR (Classless Interdomain Routing) que también es una sumarización que agrupa redes clase A y B en una sola, así como las clases C.

El CIDR no realiza ruteo classful (ruteo de acuerdo a la clase del numero de red), su ruteo es del tipo classless ya que rutea según los bits de orden superior de la dirección IP que se denominan prefijo IP.

Las mascaras ya no están restringidas a /8, /16 y /24 bits correspondientes a las clases A, B y C respectivamente.

En esta técnica al igual que en la sumarización la operación que se realiza agrupa direcciones de red de acuerdo a un prefijo común a nivel binario y a este mismo nivel los bits considerados de orden común serán los que definan en igual cantidad de numero a la mascara de red, Fig. 3.3.4.2

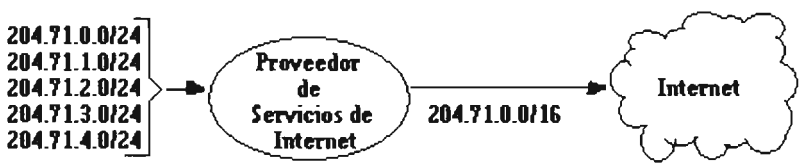


Fig. 3.3.4.2 CIDR

CIDR maneja el ruteo para un grupo de redes con un prefijo común como una sola entrada de ruteo. Es por ello que múltiples números de red de clase C asignados a una sola organización tiene un prefijo común. Cada entrada de direccionamiento CIDR contiene una dirección IP de 32 bits y una mascara de red de 32 bits que en conjunto dan la longitud y valor del prefijo IP esto se puede representar como:

<Dir_IP mascara _red>

CIDR resuelve el problema de la explosión de la tabla de ruteo para no tener que incluir información acerca de cada una de las redes de destino clase C que se pudieran adquirir. En vez de ello CIDR incluye en las tablas de información de ruteo, información acerca del tamaño de los bloques y el numero de bloques, así, en las tablas de ruteo IP se tienen pares (destino, router) donde destino no es una dirección de host o red tradicional sino que incluye información acerca del numero de redes que incluye el bloque y el tamaño de cada una de esas redes.
CIDR debe incluir en las tablas de ruteo cual es la primera red que compone el bloque, cuantos bits se emplean como prefijo de red y la mascara de subred que se emplea.
Por ejemplo el par <194.0.0.0 254.0.0.0> representan el prefijo de 7 bits 1100001
Para el caso dela Fig. 3.3.4.1 el par <204.71.0.0 255.255.0.0> representa el prefijo de 16 bits 11111111 11111111. Como se puede ver los bits que componen la mascara para este prefijo es menor que los bits de la mascara de las direcciones de entrada, asimismo podemos ver que las 5 direcciones de entrada se pueden representar en la tabla de ruteo como una sola gracias al CIDR. CIDR maneja el encaminamiento para un grupo de redes con un prefijo común con una sola entrada de encaminamiento. Esta es la razón por la que múltiples redes de clase C asignadas a una sola organización tienen un prefijo comun.
Al proceso de combinar múltiples redes en una sola entrada se le llama agregación de direcciones o reducción de direcciones. Esto también es conocido como supernetting por que el ruteo se basa en mascaras de red más cortas que la mascara de red natural de la dirección IP, en contraste con el subnetting donde las mascaras de red son mas largas que la mascara natural. También en subnetting las mascaras de subred pueden ser contiguas pero pueden tener una parte local no contigua y las mascaras de superred son siempre contiguas.
En esta técnica la mascara de red puede decrementar en numero de bits cuando se presenta en redes clase C. Debido a esto la sumarización se aplica mas a redes clase A y B y el CIDR se aplica a redes clase C.
Un aspecto muy importante de CIDR es que en ningún momento cambia el algoritmo básico de enrutamiento IP, lo que cambia es el contenido de las tablas. Además las nuevas tablas contienen información resumida, por lo que buscar una dirección destino en la tabla se hace de otra manera, pero el algoritmo permanece inalterado.
CIDR permite realizar la agregación de direcciones muy eficientemente gracias a la topología de encaminamiento en forma de árbol donde cada hoja del árbol representa un dominio de encaminamiento y el esquema de direccionamiento se elige de modo que cada bifurcación del árbol corresponde a un incremento en la longitud del prefijo IP. Si un router en Norteamérica encamina todo el trafico europeo a través de un único enlace, entonces una sola entrada de encaminamiento de <194.0.0.0 254.0.0.0> incluirá el grupo de direcciones de redes de clase asignadas a Europa.
La filosofía de CIDR usa un lema (la mejor aproximación es la que tiene mas aciertos) por lo que sí se quiere hacer una excepción para el rango de direcciones de Europa de las 64 representadas por el par <195.1.64.0 255.255.192.0> se necesitara solo una entrada adicional que en la tabla se superpone a otras entradas mas generales (mas cortas de las redes que contiene). Con este ejemplo se puede ver que a medida que aumenta el uso del espacio de direcciones clase C, los beneficios de CIDR aumentan por igual, siempre que la asignación de direcciones siga la topología de red. Pero el estado actual del espacio de direcciones IP no sigue este esquema debido a que el desarrollo de CIDR fue posterior, sin embargo se están asignando nuevas direcciones IP compatibles con CIDR lo que deberá aliviar un poco el problema de la explosión de las tablas de ruteo a corto plazo aunque a

largo plazo puede ser necesaria una reestructuración del espacio de direcciones de acuerdo a pautas topológicas, lo que supone un enorme trabajo de renumerar un gran numero de redes.

Esta forma de asumir la topología de ruteo como un árbol es un exceso de simplificación ya que muchos dominios no tienen un solo enlace a Internet conocidos como unipuerto (single-homed) sino tienen múltiples enlaces conocidos como multipuerto (multi-homed), además de esto la topología no es estática ya que se unen nuevas organizaciones constantemente y de las ya existentes muchas cambian su topología por ejemplo al cambiar de proveedor de Internet. Estos casos complican la implementación de CIDR y reducen su eficiencia.

Las políticas para la distribución de direcciones IP con CIDR son:

- La asignación de direcciones IP refleja la topología física de la red y no la de la organización, las restricciones organizacionales y administrativas no deberían usarse en la asignación de direcciones IP cuando no se ajusten a la topología de la red.
- Las direcciones IP se deberían asignar partiendo de la base de que la topología de la red seguirá de cerca los limites continentales y nacionales.
- Habrá un numero relativamente pequeño de redes que transportaran una elevada cantidad de trafico entre dominios de encaminamiento y que estarán conectadas de modo no jerárquico, traspasando los limites nacionales. Estas redes se conocen como TRDs (Transit Routing Domain). Cada TRD tendrá un prefijo IP univoco, no se organizaran jerárquicamente y cuando se halle dentro de los limites continentales, su prefijo debería ser una extensión del prefijo IP continental.
- Se pueden ignorar las conexiones privadas que no tienen efecto significativo en la topología de la red como las organizaciones con enlaces a otras organizaciones que no transportan trafico dirigido a otros dominios (trafico de transito).
- La mayor parte de los dominios de encaminamiento serán single-homed debido a que están conectados a un solo TRD. A esos dominios se le debería asignar direcciones que comiencen por el prefijo IP de ese TRD. Por tanto todas las direcciones de los dominios single-homed conectados a un TDR se pueden agregar en una sola entrada de la tabla de ruteo para todos los dominios externos a ese TDR. Esto provoca que si una organización cambia su proveedor de servicios de Internet deberá cambiar todas sus direcciones IP.

Algunos esquemas de asignación de direcciones para dominios multi-homed son:

- Uso de un único prefijo IP para el dominio. Los routers externos deben tener una entrada para la organización que se halla parcial o totalmente fuera de la jerarquía normal. Donde un dominio sea multi-homed, pero todos los TDRs conectados están topologicamente cerca, seria apropiado que el prefijo IP del dominio incluyese los bits comunes a todos los TRDs conectados.
- El uso de un prefijo IP para cada TRD conectado, con hosts en el dominio que tengan direcciones IP que contengan el prefijo del TRD mas apropiado. La organización da la impresión de ser un conjunto de dominios de ruteo.
- Asignar un prefijo IP de uno de los TRDs conectados. Este TRD se convierte en un TRD por defecto para el dominio, aunque otros dominios puedan encaminar explícitamente sus mensajes por uno de los TRDs alternativos.
- El uso de prefijos IP para referirse a conjuntos de dominios multi-homed con conexiones a TRDs. Por ejemplo puede haber un prefijo IP que se refiera a dominios

single-homed conectados a la red A, un prefijo que se refiera a dominios single-homed conectados a la red B y uno para los dominios conectados a A y a B.

Implementación de CIDR

La implementación de CIDR en Internet se basa en el protocolo BGP (Border Gateway Protocol, versión 4), también se implementa con una variante del ISO IDRP conocida como IDRP par IP.

La estrategia de implementación que se describe en el RFC 1520 Intercambiando información de ruteo a través de las fronteras de los proveedores en el entorno CIDR se realiza en fases a través de la jerarquía de ruteo empezando por los routers troncales. Los proveedores de servicios de red se dividen en cuatro tipos:

Tipo1. Aquellos que no pueden emplear ningún tipo de IDRP.

Tipo 2. Los que usan IDRP por defecto pero que requieren rutas explícitas para una proporción considerable de los números IP de red asignados.

Tipo 3. Los que usan IDRP por defecto y añaden además un pequeño numero de rutas explicitas.

Tipo 4. Los que ejecutan IDRP utilizando solo rutas por defecto.

La implementación de CIDR implica una primera fase por medio de los proveedores de tipo 0, luego los de tipo 2 y finalmente los de tipo 3. CIDR ya se ha aplicado ampliamente en troncales y más de 9000 rutas se han reemplazado por aproximadamente 2000 rutas CIDR.

En resumen las características de CIDR son:

- Es el único método reconocido como supernetting estándar.
- El método reduce el crecimiento de las tablas de ruteo.
- Sumariza múltiples direcciones de red en un numero más pequeño de entradas en las tabla de ruteo.
- Múltiples direcciones IP a ser sumarizadas deben compartir el mismo prefijo o bits de mayor orden.
- Las tablas de ruteo y los algoritmos ahora deben basar sus decisiones de ruteo sobre una dirección IP de 32 bits y una mascara de 32 bits.
- Los prefijos de red estándar eran de 8, 16 y 24 bits, ahora los prefijos de CIDR son de entre 13 y 27 bits.
- Los bloques de direcciones se pueden asignar a redes pequeñas (32 hosts) hasta redes muy grandes (50,000 hosts).
- Una dirección CIDR incluye la dirección IP de 32 bits estándar y también información de cuantos bits son usados por el prefijo de red.

Por ejemplo los rangos de redes privadas con CIDR tendrán las nuevas mascaras mostradas en la tabla 3.3.4.2

Inicio	Final	Notación CIDR
10.0.0.0	10.255.255.255	10.0.0.0/8
172.16.0.0	172.31.255.255	172.16.0.0/12
192.168.0.0	192.168.255.255	192.168.0.0/16

Tabla 3.3.4.2 Notación de las redes privadas mediante CIDR

NAT

Una solución que trata de ayudar a optimizar la utilización de las direcciones asignadas por IANA es la técnica introducida por Cisco conocida como traducción de direcciones de red NAT (Network Address Translation). Esta técnica permite usar los bloques de direcciones privadas que no son son ruteables en Internet. NAT transforma los esquemas de direcciones intranet no ruteables en esquemas únicos de direcciones globalmente ruteables.

La función NAT se procesa en el ruteador que se encuentra entre el esquema de direcciones privado y el esquema de direccionamiento público exterior, lo que permite un acceso transparente a Internet por parte de los nodos de la intranet. NAT elimina el significado extremo a extremo que utiliza el protocolo IP para usar TCP que establece una conexión para cada salto, permitiendo así el cambo de direcciones de la conexión TCP.

La técnica NAT permite realizar el mapeo de las direcciones privadas usando un pool de direcciones IP homologadas para poder tener comunicación con Internet como muestra la Fig. 3.3.4.2

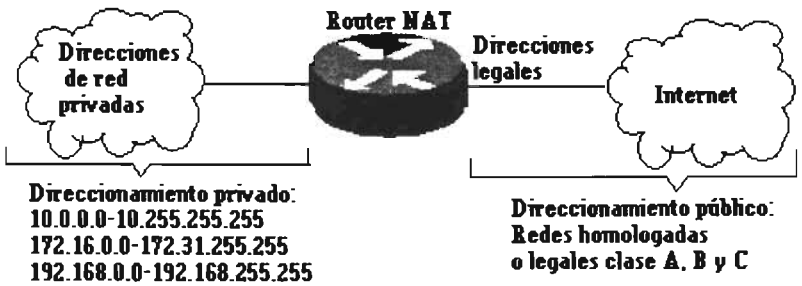


Fig. 3.3.4.2 Conexión a Internet mediante uso de NAT

Por lo tanto la técnica NAT se puede usar para:

- Ocultar una dirección IP interna de red por razones de seguridad.
- Para usar una dirección IP no valida en una red interna para conectarse a Internet.
- Para hacer un redireccionamiento para un ruteo mejorado.
- Realizar un mapeo de uno-a-uno necesario para servidores
- Traducción mediante un pool de direcciones
- Traducción a una sola dirección

De esto se deduce que las otras clases de direcciones (A, B, C) no se pueden configurar en redes con acceso a Internet, aunque si la red no tiene contacto directamente con Internet se le puede configurar cualquier clase.

3.3.5 Ruteo

La función más importante del protocolo IP es el ruteo o encaminamiento

Ruteo (Routing) es el proceso de encaminar paquetes de información hasta una estación destino, usando el nivel de Internet de TCP/IP para interconectar distintas redes físicas.

Las tareas de ruteo son implementadas por el protocolo IP sin que los protocolos de nivel superior como TCP o UDP tengan conocimiento de ello. Cuando se quiere enviar

información por Internet de una maquina a otra el protocolo IP comprueba si la maquina destino se encuentra en la misma red local que la maquina origen si es así se enviara el datagrama de forma directa ya que la cabecera IP contienen el valor de la dirección Internet y la cabecera Ethernet contiene el valor de la dirección de la red física (Ethernet) que corresponde a la maquina destino.
Cuando se pretende enviar información a una maquina que se encuentra en otra red distinta a la de la maquina origen el proceso es un poco más complicado, para esto se tiene que realizar un ruteo indirecto y es el caso que se presenta mas frecuentemente cuando se envía información en Internet. Internet forma una gran red lógica que interconecta diferentes redes de diferentes tamaños gracias a la funcionalidad del protocolo IP. En Internet existe un elevado numero de redes independientes conectadas entre sí mediante routers (ruteadores).

Ruteo IP básico
Un router básico con información parcial de ruteo solo contiene información acerca de cuatro tipos de destino:

- Los hosts conectados a una de las redes físicas a las que esta conectado el router.
- Los hosts o redes para los que se ha dado al router información especifica.
- Los hosts o redes para las que el router ha recibido un mensaje ICMP redirect.
- Un destino por defecto para todo lo demas.

Los dos últimos casos permiten a un router básico comenzar con una cantidad muy limitada de información para irla aumentando debido a que un router más avanzado lance un mensaje ICMP redirect cuando reciba un datagrama y conozca un router mejor en la misma red al cual dirigir el datagrama. Este proceso se repite cada vez que un router básico se reinicia.
La función fundamental del ruteo esta presente en todas las implementaciones de IP. Cuando un datagrama entrante que especifica una dirección destino distinta a la dirección local del host estará sujeto al algoritmo de ruteo IP del host local, que selecciona el siguiente salto del datagrama (siguiente host al que se enviara). El nuevo destino puede estar en cualquiera de las redes físicas con las que el host esta conectado. Si es una red física diferente de aquella en la que se recibió el datagrama, el host intermediario entre las redes físicas retransmite el datagrama, Fig. 3.3.5.1.

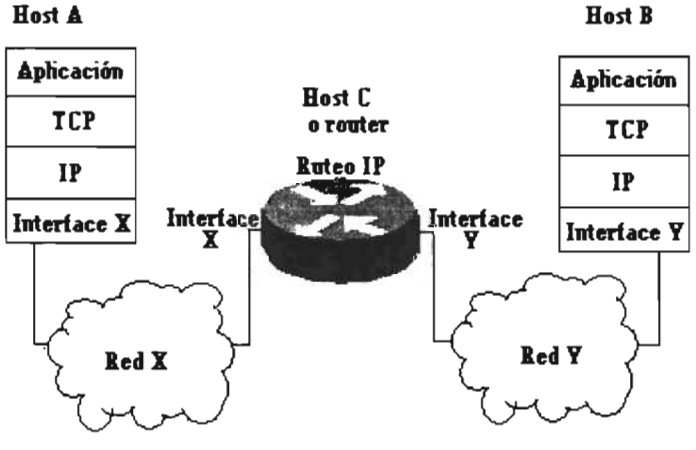


Fig. 3.3.5.1 Funcionamiento del router en IP.

La tabla de ruteo IP normal contiene información acerca de las redes conectadas localmente y de las direcciones IP de otros routers localizados en ellas, además de las redes con las que están conectados. Se puede extender con información de las redes IP que se hallan aun más lejos y tener incluso una ruta por defecto.
Con los routers básicos se tienen las siguientes consideraciones:

- No conocen todas las redes de Internet.
- Permiten la autonomía de sitios locales para establecer y modificar rutas.
- Una entrada de ruteo errónea produce inconsistencia haciendo parte de la red inalcanzable.

Un router más avanzado se requiere cuando:

- Ha de conocer las rutas a todas las posibles redes IP.
- El router ha de tener tablas de ruteo dinámicas, que se actualizan con poca o ninguna intervención manual.
- El router ha de anunciar los cambios locales a los otros routers.

Tipos de ruteo
El ruteo o enrutamiento de datagramas IP se refiere al proceso de determinar la trayectoria que un datagrama debe seguir para alcanzar su destino. Los dispositivos que pueden elegir las trayectorias se les denomina enrutadores. Existen dos tipos de enrutamiento:

- Enrutamiento directo: Es cuando se transmiten datagramas IP entre dos equipos de la misma red física sin la intervención de gateways, el proceso en este tipo de enrutamiento es muy eficiente. El emisor encapsula el datagrama IP en la trama de red, efectuado la vinculación entre la dirección física y la dirección IP por medio del protocolo ARP y envía la trama resultante en forma directa al destinatario.
- Enrutamiento indirecto. Este tipo de ruteo ocurre cuando el host destino esta en otra red distinta a la del host fuente. La única forma de hacer llegar la transmisión del datagrama hasta el destino se efectúa mediante la intervención de gateways. La dirección del primer gateway (el primer salto) se llama ruta indirecta. La dirección del primer salto es la única información que necesita el host fuente, ya que el router que reciba el datagrama se responsabiliza del segundo salto y así sucesivamente. Los gateways forman una estructura cooperativa, interconectada. Los gateways se envían los datagramas hasta que se alcanza a la compuerta que puede distribuirla en forma directa a la red destino. Los gateways que actúan como enrutadores deben estar provistos de mecanismos para conocer y decidir la trayectoria de la red que se desea alcanzar. En este tipo de ruteo, el funcionamiento en forma genérica es de la siguiente forma: El equipo que origina la información envía a un gateway el datagrama con destino a una red física distante. El gateway de la red física envía el datagrama a otras compuertas hasta alcanzar al gateway que pueda emitirlo en forma directa a la red destino. El gateway debe conocer las rutas hacia las diferentes redes externas, esas redes pueden usar a su vez un enrutamiento indirecto en el caso de no conocer la ruta a una red especifica. Los gateways almacenan las trayectorias a otras redes mediante sus tablas de ruteo.

El host puede distinguir si una ruta es directa o indirecta examinando el numero de red y subred (Net ID y SubNet ID) de la dirección IP, entonces:

1. Si coinciden algunos de los dos NetID o SubNet ID con una de las direcciones IP del host fuente la ruta es directa. El host necesita ser capaz de direccionar el destino

usando un protocolo inferior a IP, esto se hace automáticamente usando el protoloco ARP que se usa en LANs con broadcast.

2. Si no coinciden ni el NetID ni el Subnet ID la ruta es indirecta y lo único que necesita saber es la dirección IP de un router que conduzca a la red de destino.

Un ruteador puede enviar y recibir información de los hosts de todas las redes a las que esta conectado y siempre será de forma directa. Si solo se fuera a enviar información de forma directa dentro de una misma red no seria necesario el uso del protocolo TCP/IP, ya que es especialmente indicado cuando se desea comunicación con otras redes. En este caso los datagramas tendrán que ser encaminados a través de un router para llegar a su destino. La forma de hacer esto es a través del protocolo IP, el cual decide si la información puede enviarse directamente o si por el contrario debe utilizarse el método indirecto a través de un router.

Como Internet posee múltiples enlaces con diferentes redes y más de un router, cada router debe poseer una tabla donde se relaciona cada una de las redes existentes con el router que debe usarse para tener acceso. Los routers indicados en estas tablas pueden no estar conectados directamente a las redes con los que están relacionados, sino que lo que se indica es el mejor camino para acceder a cada una de ellas. Cuando un router recibe un paquete que debe ser encaminado busca en su propia tabla de redes la entrada correspondiente a la red para entregarlo al host destino. La búsqueda en la tabla puede dar como resultado la dirección de un nuevo router al cual dirigir el paquete y así continuara el proceso sucesivamente hasta encintrar el destino final.

Los ruteadores proporcionan servicios para seleccionar una ruta basándose en parámetros como, la latencia de los enlaces, el estado de congestión de la red, la distancia entre nodos etc. de modo que puedan aplicar diferentes políticas según los requerimientos de cada aplicación, permitiendo topologías descentralizadas y complejas en base a esquemas de direccionamiento. Algunas de las funciones que los ruteadores tienen que realizar son:

- Elegir el camino más adecuado: Basados en tablas de información de los enlaces toman las decisiones para realizar el enrutamiento.
- Implementar el control de flujo: Cuando redes más rápidas saturan a las más lentas el ruteador envía una señal de congestión a la fuente indicándole que reduzca la velocidad de transmisión.
- Unir redes heterogéneas: Pueden conectar redes de diferente nivel MAC.

Los ruteadores tienen una función de forwarding (retransmisión con las siguientes características:

- La función de forwarding se encarga de encaminar los paquetes consultando a la tabla de ruteo.
- La consulta a la tabla de ruteo se realiza paquete a paquete.
- En la tabla de ruteo se indica para cada destino, el siguiente router (próximo salto) al que debe enviarse el paquete.
- Se puede usar una memoria cache para aumentar el performance de la función de forwarding.

La función de ruteo básicamente la realizan los equipos ruteadores, los cuales deben ser direccionados explícitamente, esto es, las estaciones deben conocer las direcciones de los mismos para poder comunicarse con nodos remotos. Las características de la función de ruteo son:

- La función de ruteo se encarga de construir la tabla de ruteo.

- La tabla de ruteo puede ser estática o dinámica.
- Para la actualización dinámica se utilizan protocolos de ruteo que intercambian información entre los routers de la red y utilizan algoritmos para establecer el contenido de la tabla.
- La actualización de la tabla se realiza periódicamente a intervalos del orden de decenas de segundos.
- Los protocolos de ruteo dinámicos intercambian información entre equipos usando protocolos de capas superiores.

En todos los routers que forman una red debe existir una convergencia. La convergencia ocurre cuando todos los ruteadores tienen la misma perspectiva de la topología de red. Por lo que cuando hay un cambio de topología los ruteadores deben recomputar las rutas, el proceso y tiempo requerido para la reconvergencia del ruteo varia según el protocolo de ruteo.

El proceso de ruteo requiere que se den tres condiciones:

- Mecanismo de enrutamiento: Son las actividades que un nodo o host realiza para determinar como se manejara un paquete en base a una dirección destino.
- Protocolo de enrutamiento: Es el conjunto de reglas que siguen los ruteadores para compartir información de la red para tomar decisiones.
- Tabla de enrutamiento: Contiene información acerca de los posibles destinos sobre la base de direcciones de red especificas. Las tablas de enrutamiento pueden ser creadas y actualizadas en base a 4 modos:
  1. Directamente conectadas. Son rutas hacía direcciones de red conectadas directamente a las interfaces del ruteador.
  2. Estáticamente: Son creadas mediante un procedimiento manual largo y tedioso por los administradores de la red. Las rutas se fijan en función de la capacidad de la línea, el trafico medio u otros criterios similares, estas rutas indican el router al cual enviar los paquetes. Como se cargan las tablas de ruteo de forma estática no se necesita intercambiar información con los vecinos y por lo tanto no se requiere un protocolo de ruteo. El ruteo estático no puede responder a situaciones cambiantes como saturación, exceso de trafico o fallo de una línea.
  3. Dinámicamente: Para esto usan un ruteo dinámico donde los routers intercambian información entre ellos sobre las redes que tienen conectadas. Usan algoritmos automáticos (daemons) más fáciles de configurar, pero el overhead de la red aumenta por los continuos intercambios de control de información entre ruteadores y recopilación en tiempo real sobre el estado de la red que se actualiza constantemente mediante paquetes que intercambian los ruteadores a través de la misma red. Las rutas optimas se recalculan continuamente en función de la información que los ruteadores reciben en tiempo real sobre el estado de la red. Se utilizan algoritmos autoadaptivos y es preciso utilizar un protocolo de ruteo que permita a los ruteadores intercambiar continuamente esa información. Los algoritmos no pueden ser demasiado complejos ya que deben implementarse en los ruteadores y ejecutarse en tiempo real con los recursos de CPU y memoria de que el ruteador dispone.
  4. Por omisión. Son rutas hacia otro gateway que conoce las rutas a la dirección de red destino.

La forma más común de ruteo requiere el uso de una tabla de ruteo IP, presente tanto en los hosts como los routers. Estas tablas no pueden contener información sobre cada posible destino. En vez de ellos se aprovecha el esquema de direccionamiento IP para ocultar detalles acerca de los hosts individuales, además las tablas no contienen rutas completas, sino solo la dirección del siguiente paso en esa ruta.
En general una tabla de ruteo IP tiene pares (destino, router), donde destino es la dirección IP de un destino particular y router es la dirección del siguiente router en el camino hacia ese destino. El router debe ser accesible directamente desde la maquina actual. Por su naturaleza estática este tipo de ruteo tiene varias consecuencias:

1. Todo el trafico hacia una red particular toma el mismo camino, desaprovechando caminos alternativos y el tipo de trafico.
2. Solo el router con conexión directa al destino sabe si existe o esta activo.
3. Es necesario que los routers cooperen para hacer posible la comunicación bidireccional.

3.3.6 Protocolos de ruteo

El encaminamiento (ruteo) forma parte de la capa de red, pero la función principal de un protocolo de ruteo es intercambiar información con otros routers, y en este sentido los protocolos se comportan como si fueran protocolos de la capa de aplicación. Todos los protocolos escritos aquí emplean tres estrategias para el transporte de datos: transporte mediante UDP (por ejemplo RIP), transporte mediante TCP (BGP) o bien crea su propia capa de transporte sobre IP (OSPF).
Para facilitar el mantenimiento de las tablas de ruteo existen algunos protocolos para ruteo que permiten que un router o gateway cualquiera pueda encontrar por si mismo la localización de otros routers o gateways y guardar la información acerca del mejor camino para acceder a cada red.
Los protocolos de ruteo son procedimientos o procesos que optimizan las trayectorias preestablecidas en los paquetes de datos, para ello utilizan una métrica, un algoritmo y daemons, con la combinación de estas tres características optimizan las trayectorias preestablecidas en los paquetes de datos. En base al adecuado manejo de estos parámetros los protocolos harán converger las redes más rápida o lentamente. La convergencia en el sentido de ruteo se refiere al aspecto de que todos los elementos de las redes actualizan sus tablas de ruteo.
El protocolo de ruteo hace a un router completamente funcional para poder intercambiar información con otros routers en redes remotas, proporcionándole información como:

- Topología.
- Condiciones de falla.
- Métricas de costo del enlace (cuenta de saltos, ancho de banda, retardo etc.).
- Confiabilidad de la ruta.
- Utilización del enlace.

Algunos conceptos importantes que manejan los protocolos de ruteo son:

- Ruteo classful y ruteo classless.
- Métrica.
- Sistema autónomo.

- Distancia administrativa.

Ruteo classful y ruteo classless
Los ruteadores cuándo se interconectan comienzan a comunicarse entre sí para intercambiar las direcciones de red de las rutas que ya han conocido y con esta información actualizan sus tablas de ruteo a intervalos determinados. El anunciamiento de sus direcciones lo hacen de dos maneras:

- Classless: Anuncian la dirección de red junto con la mascara de red.
- Classful: Anuncian la dirección de red sin anunciar la mascara de red.

Métrica
La métrica es un parámetro que el protocolo de ruteo usa para determinar la trayectoria más viable u optima en ese momento para establecer la trayectoria virtual (Vp) y posteriormente el canal virtual (Vc), para el transporte de paquetes basándose en la comparación entre rutas.

Algoritmo
Un algoritmo es el conjunto de reglas y procedimientos del proceso.

Sistema autónomo
La red Internet se divide en sistemas autónomos. Un sistema autónomo (AS) es un dominio de administración lógico que se compone de routers y grupos de redes administrados por una sola autoridad. Un AS, utiliza un mismo protocolo interno (IGP) de distribución y actualización de la información de ruteo. Los SA se conectan entre sí mediante routers externos que utilizan un mismo protocolo externo (EGP).
Los AS pueden ser numerados o no dependiendo del protocolo que lo utilice. Cada numero que identifica al AS es de 16 bits y es asignado por las autoridades de numeración. Todas las partes de un AS deben permanecer conectadas. La división de Internet en AS pretende disminuir el exceso de encabezado de ruteo. El AS tiene un protocolo de ruteo homogéneo mediante el cual intercambia información en todo el dominio y posee una política común para el intercambio de información con otras redes o AS.

Distancia administrativa
Es un valor adimensional que se utiliza para el calculo de rutas determinando que protocolo de ruteo o bien que elemento de hardware o software es más confiable. Es usado para decidir cuando se tienen dos o más rutas para llegar a un destino. A menor distancia administrativa mayor confiabilidad.

Routing daemons
Los routing daemons son procesos o subrutinas que tienen como finalidad, llevar a cabo las instrucciones que un protocolo de ruteo utiliza para realizar el calculo de la métrica y demás parámetros que necesita para determinar la mejor trayectoria que seguirán los paquetes. El proceso daemon se encarga de agregar, borrar o actualizar la tabla de ruteo según el estado de la red, además de determinar la política de ruteo. En general los daemons son procesos autónomos que se autoejecutan.

Convergencia

Cuando todos los dispositivos de ruteo han actualizado todas sus tablas de ruteo, se dice que ha habido convergencia de ruteadores. Cuando todos los dispositivos integrantes de la red han actualizado todas sus tablas, se dice que ha habido convergencia de la red. La convergencia siempre esta en constante actualización y nunca es absoluta.

Tablas de ruteo

Las tablas de ruteo IP es un conjunto de mapeos entre las direcciones IP de destino y las direcciones IP del siguiente salto para ese destino que cada host almacena.

La formación de tablas de ruteo se realiza mediante el uso de un algoritmo comúnmente usado para el enrutamiento de IP. Las tablas de ruteo están presentes en todo equipo que almacene información de cómo alcanzar posibles sitios. En las tablas no se almacena la ruta especifica a un equipo, sino aquella a la red donde se encuentre. Para esto cada puerto de comunicación del gateway debe tener una dirección IP.

Las tablas de ruteo juegan un papel fundamental para el envío de paquetes. Cada router y cada host tendrá su tabla de ruteo. Una vez conocida la dirección IP destino la tabla permitirá decidir cual es el próximo ruteador al que debe enviarse el paquete.

Las tablas de ruteo tendrán dos columnas fundamentales: la primera contendrá los destinos, la segunda indicará el siguiente salto. Se tiene dos tipos de entradas, las entradas correspondientes a las subredes de las cuales el host o router forma parte y las entradas correspondientes a otras subredes. En el primer caso la tabla indicara la interfaz de red que debe utilizarse, mientras que en el segundo caso indicara la dirección IP del router que continuara la tarea. Dada una dirección IP destino se buscara en la tabla una entrada que contenga dicha dirección. En caso de que exista mas de una, tomara aquella con la que coincidan mas bits (mascara con mas 1´s) Existe la posibilidad de configurar una entrada default, indicando la ruta pro defecto para el caso en que no exista una entrada mas especifica.

Para que la tabla no sea excesivamente grande, que contenga todas las rutas a las redes que interconecta el equipo, es necesario que con un minino de información el equipo pueda tomar decisiones de ruteo, para esto se puede usar la técnica de mantener tablas de ruteo pequeñas enviando los datagramas a destinos predeterminados. Para ello es de gran utilidad definir una ruta por default. A través de esa ruta se deben alcanzar todas las redes destino.

La ruta por default apunta a un dispositivo que actúa como gateway de la red donde se encuentra ubicado el equipo que la posee.

Las tablas de ruteo pueden contener tres tipos de mapeo:

1. Rutas directas, para redes conectadas localmente.
2. Rutas indirectas, para redes accesibles a través de uno o más routers
3. Una ruta por defecto, que contiene la dirección IP de un router que todas las direcciones IP no contempladas en las rutas directas e indirectas han de usar.

Los protocolos de ruteo son dinámicos, el ruteo dinámico realiza peticiones de comunicaciones para que las rutas sean calculadas automáticamente a intervalos regulares por software en dispositivos de ruteo. Esto contrasta con el ruteo estático donde en los routers las rutas son establecidas por el administrador de red y no cambian hasta que este las cambia.

Una tabla de ruteo IP que consiste de pares (dirección destino/siguiente salto) es usada para habilitar el ruteo dinámico.

El ruteo IP especifica que los datagramas IP viajen a través de las redes conectadas un salto a la vez, sin embargo la ruta completa no es conocida al principio de la jornada. Sin

embargo en cada salto, el siguiente destino es calculado haciendo corresponder la dirección destino dentro del datagrama con una entrada en la tabla de ruteo del nodo actual.
Cada nodo involucrado en el proceso de ruteo esta limitado a la retransmisión de paquetes basado en la información interna. Los nodos no monitorean si los paquetes llegan a su destino final, ni IP regresa reportes de error a la fuente cuando el ruteo anormal ocurre, esta tarea es dejada a otro protocolo de Internet, el protocolo ICMP.

Propagación automática de rutas
Conforme las complejidades de las redes aumentaron se busco un mecanismo que propagara la información de rutas entre compuertas de forma automática debido al cambio dinámico de las redes, esto para evitar que las transiciones entre gateways resultara lenta y no reflejara el estado de la red en un momento dado. Para ello se han establecido algoritmos para el intercambio de información entre gateways.
Los protocolos de ruteo implementan un algoritmo de camino más corto entre los ruteadores en base a una métrica como puede ser la cantidad de saltos o nodos atravesados hasta alcanzar el destino, algún tipo de costo asignado a cada interfaz de red. Según el método usado para calcular el camino mas corto o el camino de menor costo y según la forma de intercambiar las rutas entre los ruteadores se distinguen dos tipos de protocolo por el algoritmo utilizado para determinar el ruteo:

- Algoritmo por vector distancia o de Bellman-Ford.
- Algoritmo de estado de enlace o Shortest Path First.

Un algoritmo de ruteo es el conjunto de direccionamientos y subrutinas que un protocolo de ruteo utiliza para realizar el calculo de la métrica y demás parámetros que necesita para determinar la mejor trayectoria que seguirán los paquetes.

Algoritmo de estado de enlace
Este algoritmo es el mejor en términos de estabilidad, velocidad de actualización, manejo de overhead, etc. por lo que es el mas usado. Con este algoritmo cada ruteador informa los costos de cada una de sus interfaces a todos los ruteadores de la red. Así todos los ruteadores tienen un conocimiento completo de la topología de la red y pueden ejecutar localmente un algoritmo de camino mas corto o de menor costo para determinar el contenido de sus propias tablas de ruteo.
En general el funcionamiento del algoritmo de estado de enlace es el siguiente: Cada router envía periódicamente una descripción de su conexión (el estado del enlace) a sus vecinos (aquellos conectados a la misma red) Esta descripción llamada LSA (Link State Advertisement), incluye el costo de la conexión. El LSA inunda el dominio del router. Cada router del dominio mantiene una copia idéntica y sincronizada de una base de datos compuesta de la información del estado del enlace. La base de datos describe la topología del dominio, como las rutas a redes en otros AS. Cada router ejecuta un algoritmo sobre su base de datos resultando en un árbol del camino mínimo (MST o Minimum Spanning Tree), que contiene la ruta mas corta por router y red que pueda alcanzar el gateway. A partir del costo hacia el destino y el salto siguiente para retransmitir un dato se utilizan para construir la tabla de encaminamiento del router.
Después del primer flood inicial y habiendo alcanzado la sincronización o convergencia entre ruteadores vecinos, solamente pasa pequeñas actualizaciones del estado del enlace generadas por cambios o eventos a todos los ruteadores. Este tipo de algoritmos en comparación con los de vector distancia envían actualizaciones cuando hay noticias que

pueden ser regulares para asegurar a los vecinos que la conexión sigue activa. Aquí lo importante es que la información intercambiada es el estado del enlace, no los contenidos de la tabla de ruteo. Estos algoritmos usan menos recursos que los de vector distancia, sobre todo cuando el ruteo es complejo o el AS es grande. Sin embargo tienen un elevado costo computacional. A cambio se consigue respuesta a los eventos de red más rápido, convergencia más veloz y acceso a servicios de red mas avanzados.
Las características de este algoritmo son:

- Un conjunto de redes físicas se divide en un numero de áreas.
- Todos los routers dentro de un área tienen idénticas bases de datos.
- Obtiene una vista común de la topología entera de la red ya que cada router tiene una base de datos que describe la topología completa del dominio de ruteo (que routers se conectan a que redes). La topología de un área se representa en una base de datos llamada LSD (Link State Database) que es una descripción de todos los enlaces de los routers del área.
- Cada router usa su base de datos para derivar el conjunto de caminos mínimos a los destinos de los que construye su tabla. El algoritmo usado para determinar los caminos óptimos se llama SPF (Shortest Path First).
- Calcula el camino mas corto hacia otros ruteadores.
- Actualizaciones periódicas pero poco frecuentes (cada 30 seg.) iniciadas por eventos por lo que la convergencia es rápida.
- Transmite actualizaciones de ruteo link-state hacia otros ruteadores.
- El envío de su tabla de ruteo parcial es en forma de multicast.
- La convergencia es muy rápida por lo que se pueden usar en redes escalables.

Algoritmo de vector distancia
El termino vector-distancia se refiere a una clase de algoritmos que usan los gateways para actualizar su información de ruteo.
El algoritmo de vector distancia permite definir que tantos gateways debería viajar un paquete para alcanzar su red destino.
Se asume que cada gateway comienza su operación con un conjunto de rutas básicas de cómo alcanzar las redes que conecta directamente y posiblemente algunos routers adicionales a otras redes o hosts. Las rutas son almacenadas en tablas de ruteo que indican la red o hosts de destino y los saltos o distancia para alcanzar esa red, esta distancia se denomina métrica y se mide típicamente en saltos. Mediante el vector, un gateway puede saber a que otro gateway enviar el paquete de información, sabiendo que este podría no ser el último gateway por el que el paquete tendría que viajar. El esquema permite tener varios caminos a una misma red, eligiendo el camino mas corto, es decir el gateway que con menos saltos conduce a la red destino.
El algoritmo de vector distancia (VD) periódicamente manda copias de sus tablas de ruteo a los routers vecinos que puede alcanzar directamente y acumulan vectores de distancias. Cuando un gateway recibe el comunicado de otro gateway actualiza su tabla incrementando en uno el numero de saltos. Con este algoritmo los ruteadores descubren el mejor camino a sus destinos a través de cada vecino. Cuando tienen que anunciar subredes lo hacen en forma sumarizada. Cuando un mensaje le llega al router B del A, B examina el conjunto de destinos que recibe y la distancia a cada uno, entonces B actualizara su tabla de ruteo si:

- A conoce un camino mas corto a cada destino.
- A lista un destino que B no tiene en su tabla.

- La distancia de A a un destino desde B pasando por A ha cambiado.

Las características del algoritmo VD son:

- Ve la topología de red desde la perspectiva de sus vecinos.
- Agrega vectores distancia de ruteador a ruteador.
- Realiza actualizaciones periódicas y frecuentes por lo que la convergencia es lenta.
- Pasa copias de las tablas de ruteo a los ruteadores vecinos.

Algunas desventajas de este algoritmo son:

- Cuando las rutas cambian rápidamente, cuando aparece una nueva conexión o falla una conexión, la topología de ruteo puede no estabilizarse debido a que la información se propaga lentamente y mientras se esta propagando algunos routers tienen información de ruteo incorrecta.
- Cada router tiene que enviar una copia de toda su tabla de ruteo a cada vecino a intervalos regulares. Aunque se pueden usar intervalos más largos para reducir la carga de la red se introducirán problemas relacionados con la respuesta de la red a cambios en la topología.
- Debido a que se usa la cuenta de saltos como métrica no tiene en cuenta la velocidad o fiabilidad del enlace.
- La tarea más difícil de este algoritmo es la prevención de la inestabilidad. Para ello usa como una solución la cuenta hasta infinito representada por un valor de 16 para la red que se vuelve inestable, todos los vecinos generan un timeout y fijan la métrica de esa red a 16. Una vez que se ha producido la convergencia todos los routers tendrán una métrica de 16 para la red desaparecida. Como 16 indica infinito la red será inaccesible para todos.

En Internet se dan al menos dos niveles de ruteo, el que se realiza dentro de un sistema autónomo llamado ruteo interno o intraareas y el que se realiza entre sistemas autónomos conocido como ruteo externo o ínter áreas, Fig. 3.3.6.1

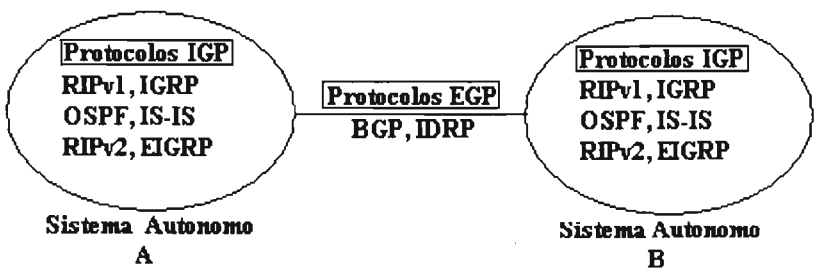


Fig.3.3.6.1 Protocolos de ruteo

Por lo que los protocolos de ruteo se dividen en:

- Protocolos de ruteo interior (intradomain) o IGP. Son los protocolos usados para realizar la función de ruteo dentro de un dominio o sistema autónomo.
- Protocolos de rueto exterior (interdomain) o EGP. Son los protocolos usados para realizar la función de ruteo entre dominios o sistemas autónomos.

- Protocolos de ruteo interior IGP.

Los protocolos de ruteo interior IGP (Interior Gateway Protocol) son usados por los routers que componen un sistema autónomo. Son de carácter técnico ya que tienen como objetivo

llegar por el mejor camino a todos los destinos dentro del AS. Los ruteadores interiores normalmente se comunican con otros, intercambian información de accesibilidad a red o información de ruteo de red (conocimiento acerca de redes dentro del sistema y redes externas), a partir de la cual la accesibilidad se puede deducir, se clasifican en tres grandes grupos según el algoritmo de ruteo que se utilice:

- Protocolos IGP con algoritmo de vector distancia:
  Dentro de esta clasificación tenemos los protocolos: RIPv1, IGRP.
- Protocolos IGP con algoritmo de estado de enlace:
  En esta clasificación tenemos a OSPF e ISIS
- Protocolos IGP Híbridos. Los protocolos híbridos combinan las características de vector distancia y estado de enlace:
  RIPv2 y EIGRP.

- Protocolos de ruteo exterior EGP.

Por su parte los protocolos de ruteo exterior EGP son de carácter político ya que hacen enrutamiento en base a políticas, llegando incluso a impedir ciertos tránsitos considerados inconvenientes. Dentro de los protocolos de ruteo exterior básicamente se encuentran:

- BGPv4.
- IDRP.

Donde el más usado es BGPv4.

- **Protocolo de ruteo interior RIP**

Existen dos versiones de RIP. La versión 1 comúnmente llamada RIP es un protocolo muy utilizado con un cierto numero de limitaciones. La versión 2 es una versión mejorada, diseñada para aliviar estas limitaciones siendo al mismo tiempo compatible con la versión 1.

El protocolo de información de ruteo RIP (Routing Information Protocol) es uno de los protocolos IGP mas ampliamente usados para intercambiar información de ruteo. Es una implementación directa del encaminamiento vector-distancia para LANs. Utiliza UDP como protocolo de transporte, cada host que usa RIP tiene un proceso de ruteo que manda y recibe datagramas sobre el puerto UDP 520 como puerto de destino.

La versión 1 de RIP no soporta mascaras de red variables CIDR, se maneja con las clases A, B y C originales, es decir es un protocolo de ruteo classful con lo que se tiene el problema de la discontinuidad de redes, la discontinuidad de redes se presenta en el momento que tenemos una red dividida en varias subredes y no pueden ser sumarizadas en una misma ruta.

El formato del paquete se muestra en la Fig. 3.3.6.2

Command	Version	Unused
Address family identifier		Route tag(only for RIP2; o for RIP)
IP address		
Subnet mask (only fro RIP2; 0 for RIP)		
Next hop (only for RIP2; 0 for RIP)		
Metric		

Fig. 3.3.6.2 Estructura del paquete RIP

- Command: se usa para especificar el propósito del datagrama, los comandos usados pueden ser:
    a. Request. Una petición al sistema correspondiente para mandar toda o parte de la tabla de ruteo.
    b. Response: Un mensaje que contienen todo o parte de la tabla de ruteo del transmisor, puede ser mandado en respuesta a una petición o consulta o puede ser un mensaje de actualización generado por el transmisor.
    c. Traceon: Obsoleto, los mensajes que contenga este comando a ser ignorados.
    d. Traceoff: Obsoleto, los mensajes que contengan este comando a ser ignorados.
    e. Reservado para SUN Microsystems.
- Versión: Numero de versión de RIP. Los datagramas se procesan de acuerdo al numero de versión, como sigue:
    a. Datagramas en los cuales él numero de versión es cero, van a ser ignorados.
    b. Datagramas cuyo numero de versión es uno, son procesados.
    c. Especifica mensajes RIP los cuales usan autenticación o transportan información en cualquiera de los campos recientemente definidos.

    >2. Datagramas cuyo numero de versión son mayores que 1 son procesados. Todos los campos que son 0 son ignorados.
- Address Family Identifier: Identifica que tipo de dirección es especificada en esta entrada particular. RIP puede transportar información de ruteo para algunos protocolos diferentes. El identificador de la familia de dirección para IP es 2. Cuando se usa autenticación el campo Address Family Identifier sera puesto a 0xFFFF. El campo etiqueta de ruta contiene el tipo de autenticación y el recordatorio del mensaje contiene el password.
- Route tag: Atributo asignado a una ruta la cual debe ser preservada y reanunciada con una ruta. La etiquete de ruta proporciona un método de separar rutas de redes dentro de un dominio RIP de rutas RIP externas, lo cual puede ser importado desde un EGP o desde otro IGP.
- IP address: La dirección IP del destino.
- Subnet Mask: Valor aplicado a la dirección IP para producir la porción no hosts de la dirección. Si es cero entonces la mascara de subred no se ha incluido para esta entrada.
- Next hop. La dirección IP del siguiente salto al cual los paquetes para el destino especificado por esta ruta serán transmitidos.
- Metric. Representa el costo total de llevar un datagrama desde el origen al destino. Es la suma de los costos asociados con las redes que serán atravesados para llegar al destino.

El protocolo RIP es un IGP basado en un vector de distancia. Si un vector conoce varias rutas para llegar a un destino, asigna un coste a la ruta en función de los saltos de gateway que deba realizar (cuantos más gateways tenga que cruzar, mas saltos deberá realizar).Cada 30 segundos envía un mensaje con su tabla de direccionamiento a los demás que actualizan sus tablas con los datos recibidos.

Los valores de los temporizadores en v1 son:

Generación de actualizaciones (respuestas): 30 segundos.

Tiempo de vencimiento de ruta =180 segundos. Se marca la ruta como expirada (metrica=16) para que los vecinos se enteren.

Tiempo de recolección de basura (garbage collection)=120 segundos. Al expirar este tiempo la ruta desaparece.
RIP es consecuencia directa de la implantación del algoritmo de vector-distancia (Bellman-Ford) para realizar el proceso de ruteo, con métrica, cantidad de saltos, cantidad de ruteadores atravesados hasta alcanzar la red destino. Es un protocolo adecuado para ruteo interno IGP para redes pequeñas, el funcionamiento de este protocolo es como se describe a continuación:
Operación básica

- En principio trabaja en uno de dos modos, divide las maquinas en activas o pasivas. Los routers activos anuncian sus rutas a los otros, las maquinas pasivas listan y actualizan sus rutas con base a estos anuncios. Solo un router puede correr RIP en modo activo de modo que un anfitrión deberá ejecutar RIP en modo pasivo.
- Cuando RIP inicia, envía un mensaje a cada uno de sus vecinos (en el puerto bien conocido 520) pidiendo una copia de la tabla de ruteo del vecino. Este mensaje es una solicitud (el campo command se pone a 1) con address family a 0 y metric a 16. Los routers vecinos devuelven una copia de sus tablas de ruteo.

Cuando RIP esta en modo activo envía toda o una parte de su tabla de ruteo a todos los vecinos (por broadcast y/o con enlaces punto a punto). Periódicamente (cada 30 seg.) se envía una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contiene toda la tabla de ruteo. La tabla consiste de pares, donde cada par contiene una dirección IP de red y un entero que representa los vectores de distancias (cuenta de saltos) hacia esa red. La tabla mantiene entradas para cada destino con su próximo salto y distancia.

- La tabla de ruteo se envía como respuesta (command vale 2 aunque no haya habido petición).
- Mantiene una tabla con una entrada por cada posible destino en la red. La entrada debe contener La distancia al destino y el siguiente salto del router a esa red.
- Cuando llega una actualización desde un vecino S, se agrega el costo asociado a la red de S cuyo resultado será la distancia D', si D' es menor que el valor actual de D se sustituye D por D'. Para mejorar el rendimiento y la fiabilidad, RIP especifica que una vez que un router (o host) ha aprendido una ruta de otro debe guardarla hasta que conozca una mejor para que no oscilen entre dos o más rutas de igual costo.
- Las rutas que RIP aprende de otros routers son borradas a menos que se vuelvan a difundir en 180 segundos. Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos y 60 segundos mas tarde se borra de la tabla.
- Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás routers

RIP por tanto hace uso de un vector de distancias, con una métrica por numero de saltos desde el origen hasta el destino, para atacar el problema del conteo al infinito se pone un limite de distancia de 16 saltos, por lo tanto el limite de saltos es 15, 16 es infinito o inaccesible. El mínimo de saltos es 1 que se utiliza para conexiones directas. El numero de saltos (hops number) o el contador de saltos (hop count) a lo largo de una trayectoria desde una fuente hacia un destino dado hace referencia al numero de routers que un datagrama

encontrará a lo largo de su trayectoria. Lo que él hace es utilizar el conteo de saltos para calcular la trayectoria optima.
Si falla un router que especifica una ruta, RIP especifica que todas las escuchas deben asociar un tiempo limite a las rutas que aprendan por medio de RIP. Cuando un router instala una ruta en su tabla inicia un temporizador para la ruta. Ese tiempo debe iniciarse cada vez que el router recibe otro mensaje RIP anunciando la ruta. La ruta queda invalidada si transcurren 180 segundos sin que el router haya recibido un anuncio nuevamente.
Cada ruteador actualiza su tabla basándose en los vectores de distancia que recibe de sus vecinos.
Mediante el uso de su algoritmo, el ruteador cada que le llega un paquete analiza su dirección destino y determina la trayectoria mas optima basándose en la distancia mas corta (menor Hop Count) que se tenga en las posibles interfaces de salida. Los saltos indican el numero de ruteadores que un paquete debe atravesar antes de llegar a su destino. Cuando se recibe una actualización de un vecino, para cada destino que aparezca en la actualización suma el costo recibido con el costo del enlace hacia el vecino, si obtiene una distancia menor o igual a la que ya tenia para el destino retiene la nueva distancia.
Usa las técnicas split horizon, poissoned reverse y triggered updates para resolver algunos problemas.
RIP debe manejar tres tipos de errores ocasionados por los algoritmos: Primeramente debe tomar precauciones para prevenir los ciclos. En segundo lugar para evitar inestabilidades debe utilizar un valor bajo para la distancia máxima posible (16). En tercer lugar el algoritmo vector-distancia crea un problema de convergencia lenta o conteo al infinito con lo cual aparecen inconsistencias debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red.
Para resolver la convergencia lenta se usa la técnica de actualización de horizonte separado (split horizon update). Con los horizontes separados el router no difunde información de rutas por la interfaz de donde fueron aprendidas. Esto ayuda a reducir la posibilidad de que lazos de ruteo se formen.
Horizontes separados a su vez usa la técnica de Poisson Reverse en la cual cuando una conexión desaparece, el router anuncia la conexión conservando la entrada de información por varios periodos de actualización e incluye un costo infinito en la difusión. Poisson reverse también anuncia las rutas por la misma interfaz donde fueron aprendidas pero con métrica al infinito.
El Poisson Reverse se hace más efectivo al combinarse con las actualizaciones activadas (Triggered Updates) que obligan al router a enviar una difusión inmediatamente al recibir malas noticias.
Este protocolo no es apropiado para redes muy grandes ya que sobre carga en exceso a los enlaces por el intercambio frecuente de las tablas de enrutamiento y debido a que solo permite 15 saltos es ineficiente para redes de gran tamaño. Normalmente no se debe implementar en redes con mas de 30 nodos. RIP funcionaba bien mientras los enlaces WAN eran de velocidad similar.
La tabla de ruteo de RIP contine los siguientes campos:

- Dirección IP destino: Es la dirección de la red final a la que se desea acceder, esta red tendrá que ser obligatoriamente classful ya que se debe tener en cuenta la clase pues no se permite el subnneting en RIPv1.

- Dirección IP del siguiente salto: Es el siguiente router por el que el paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.
- Interfaz de salida del router: Interfaz al cual esta conectado el siguiente salto.
- Métrica: Es el conteo de saltos, cada salto se considera como una única unidad, la métrica total es todos los saltos desde el router origen al destino con el limite máximo de 16.
- Temporizador: Indica el tiempo transcurrido desde que se ha recibido la ultima actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización que se establece en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos. El tiempo de actualización es el tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos. El tiempo de desactivación es el tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha mandado la actualización se considera que no esta activo en la red y se establece la métrica a 16 es decir destino inalcanzable. El tiempo de borrado es el lapso que transcurrirá una vez que el router fallo, todas las rutas de ese router son eliminadas de la tabla de ruteo.
- Banderas para indicar el estado de actualización

Algunas características de RIP son:

- Solamente soporta IP.
- Usa el algoritmo de vector distancia (Bellman-Ford).
- Envía toda su tabla de ruteo cada 30 segundos.
- La convergencia de los routers usando este protocolo es lenta.
- Es un protocolo classful, sus redes las anuncia en forma sumarizada y por lo tanto no transporta información sobre la mascara de red (versión 1).
- Su diseño es simple y su configuración es sencilla.
- No es escalable por lo que no se usa para redes grandes, máximo 30 nodos o 15 saltos.
- Su métrica esta basada en la cantidad de saltos.

Algunas limitaciones de RIP son:

- El costo máximo permitido en RIP es 16, que significa que la red es inalcanzable por lo que es inadecuando para redes grandes.
- RIP no soporta mascaras de subred de longitud variable (variable subnetting). En un mensaje RIP no hay forma de especificar una mascara de subred asociada a una dirección IP.
- Carece de servicios para garantizar que las actualizaciones proceden de routers autorizados. Es un protocolo inseguro.
- Usa métricas fijas para comparar rutas alternativas. No es apropiado para situaciones en las que las rutas necesitan elegirse en base a parámetros de tiempo real como el retardo, fiabilidad o carga.
- Depende de la cuenta hasta infinito para resolver situaciones inusuales.

- **Protocolo de ruteo interior IGRP.**

El protocolo IGRP (Internal Gateway Routing Protocol) es un protocolo creado por Cisco, es un protocolo llamado de distancia vectorial debido a que selecciona el mejor camino a través de la ponderación de un vector de métricas (mientras RIP emplea una, IGRP emplea varias) como el ancho de banda el retardo, la confiabilidad y la carga.

El protocolo IGRP (Interior Gateway Routing Protocol) tiene las siguientes características:

- Su métrica es ancho de banda (BW) y retraso (delay) de paquetes.
- Es un protocolo del tipo classful.
- Envía oda su tabla de ruteo cada 90 segundos.

El protocolo de ruteo de pasarela interior IGRP (Interior Gateway Routing Protocol) es usado para transferir información de ruteo entre routers. IGRP es mandado usando datagramas IP con IP 9 (IGP). El paquete empieza con un encabezado el cual comienza inmediatamente después del encabezado IP. Fig. 3.3.6.3

	Octetos
Version	1
Opcode	1
Edition	1
ASystem	1
Ninterior	1
Nsystem	1
Nexterior	1
Checksum	1

Fig. 3.3.6.3 Encabezado IGRP.

- Versión: Numero de versión del protocolo
- Opcode: Código de operación indicando el tipo de mensaje: 1. Actualización, 2. Petición.
- Edition: Numero serial que es incrementado cada vez que hay un cambio en la tabla de ruteo. El numero de edición permite a los gateways evitar el procesamiento de actualizaciones que contienen información que ya han visto.
- Asystem: Numero de sistema autónomo. Un gateway puede participar en mas de un sistema autónomo, donde cada sistema ejecuta su propio IGRP. Por cada sistema autónomo hay tablas de ruteo completamente separadas. Este campo permite al gateway seleccionar cual conjunto de tablas de ruteo usar.
- Ninterior, Nsystem, Nexterior: Indica él numero de entradas en cada una de estas tres secciones de mensajes de actualización.
- Checksum: La suma de comprobación IP es calculada igual que la suma de UDP, es calculada en el encabezado IGRP y cualquier información de ruteo que le sigue, no incluye el encabezado IP. El campo checksum es puesto a cero cuando se calcula la suma de comprobación.

Una petición IGRP solicita al recipiente mandar su tabla de ruteo. El mensaje de petición tiene solo un encabezado. Solo los campos Versión, Opcode y Asystem son usados. Un mensaje de actualización IGRP contiene un encabezado seguido por entradas de ruteo. Se incluyen tantas entradas de ruteo como sean posibles para ajustarse al datagrama de 1500 bytes.

- **Protocolo de ruteo interior OSPF.**

OSPF (Open Shortest Path First) es el protocolo de ruteo interior más usado actualmente, principalmente cuando se interconectan equipos de diferentes fabricantes, esta diseñado para operar con un protocolo de ruteo exterior adecuado como BGP. Su función es encontrar la trayectoria mas corta de un dispositivo de ruteo a todos los demás. Cada dispositivo de almacenamiento tiene almacenada en una base de datos la topología de la red de la que forma parte, la representación de esta topología se expresa como un grafico dirigido.

Este protocolo es complejo con el propósito de asegurar que las bases de datos topológicas son las mismas para todos los routers dentro de un área, ya que estas bases de datos son importantísimas para la toma de decisiones de ruteo.

OSPF se comunica por medio de IP (numero de protocolo es el 89). El protocolo de primero la ruta mas corta abierta OSPF (Open Shortest Path First) usa el algoritmo de estado de enlace por lo que la información de ruteo se deriva de paquetes LSA (Link State Advertisements) con el cual un ruteador prueba continuamente el estado de sus enlaces hacia cada uno de sus vecinos y envía esta información a esos mismos vecinos, los cuales hacen lo mismo para propagar la información a través del sistema autónomo o dominio, de forma tal que cada ruteador toma esta información y construye una tabla de ruteo completa de toda la red para armar la topología de conectividad de la red y a partir de allí se establece el camino mas favorable.

Es un protocolo adecuado para ruteo interno en redes pequeñas, pero se puede usar en redes grandes si se divide en áreas utilizando el ruteo jerárquico. Soporta distintas clases de redes, como redes punto a punto, de broadcast, ethernet, y de no broadcast como x.25.

OSPF realiza actualizaciones vía multicast a intervalos de 30 minutos aproximadamente o solamente cuando hay un cambio en la topología de la red por la modificación de un enlace. Exhibe las ventajas propias de los protocolos de estado de enlace: mayor estabilidad, mejor velocidad de convergencia, pero realiza un consumo mayor de procesador.

En el proceso de mandar la información de ruteo mediante un proceso de inicalización de la red un ruteador generara un mensaje de anuncio de estado de enlace (Link-state advertisement) que representa la recolección del estado de todos los enlaces de ese ruteador. Los ruteadores vecinos reciben la información guardan una copia y la retransmiten a los siguientes ruteadores con los que tiene enlaces agregando su propia información mediante un proceso de inundación (flooding).

Cuando los ruteadores quieren realizar la convergencia para descubrir a sus vecinos directos, estos envían paquetes llamados HELLO que tienen la intención de descubrir o verificar el estado de los ruteadores adyacentes. Estos paquetes HELLO son enviados por interfase cada 10 segundos.

Cuando cada ruteador tiene la información completa calcula un árbol de ruta mas corta (Shortest Path First) hacia todos su destinos con el algoritmo de Dijkstra el cual calcula para cada destino su costo y el siguiente salto para alcanzarlo.

La métrica que OSPF utiliza se define como costo que implica la relación entre la velocidad de la luz sobre un medio de fibra óptica y el ancho de banda del medio.

En OSPF se manejan áreas, donde existe un backbone conocido como área cero y todas las demás áreas deben estar físicamente conectadas al área cero posiblemente por túneles, permitiendo pasar de un área del AS a otra. Todos los ruteadores de una misma área tienen la misma base de datos de enrutamiento. Un ruteador del backbone maneja separadamente las tablas de ruteo de cada una de las áreas a las que su ruteador esta conectado.

Es un protocolo de ruteo de estado de enlace usado para rutear IP, es del tipo IGP que se usa para rutear dentro de un grupo de routers. Usa la tecnología de estado de enlace en la cual los routers mandan a cada uno de los otros información acerca de las conexiones directas y enlaces que tiene con otros routers. Ofrece un mayor grado de sofisticación con características como: Rutas basadas en el tipo de servicio, la distancia, nivel de carga, etc. Su formato es más complejo que el de RIP. Tiene una cabecera fija de 24 octetos y una parte variable para especificar el tipo de mensaje. El encabezado OSPF se muestra en la Fig. 3.3.6.4

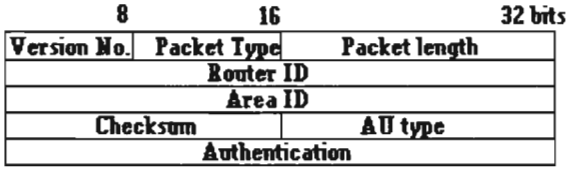


Fig. 3.3.6.4 Estructura del encabezado OSPF

- Versión number: Numero de versión del protocolo (2).
- Packet type: Tipos de paquetes: 1. Hello, 2. Descripción de base de datos, 3. Petición de estado de enlace, 4. Actualización de estado de enlace, 5.Reconocimiento de estado de enlace.
- Packet length: La longitud del paquete de protocolo en bytes, incluye el encabezado.
- Router ID: El identificador del router fuente del paquete. La fuente y el destino de un paquete de protocolo de ruteo son los dos extremos de una adyacencia.
- Area ID: Un numero de 32 bits que identifica el área a la que este paquete pertenece. Todos los paquetes OSPF están asociados con una sola área, la mayoría, lo mas que recorren es un salto. Los paquetes que viajan sobre un enlace virtual se etiquetan con el área ID principal 0.0.0.0.
- Checksum: La suma de comprobación IP estándar del contenido entero del paquete, empezando con el encabezado del paquete OSPF y excluyendo el campo de autentificación de 64 bits. Se calcula como el complemento a uno de 16 bits de la suma del complemento uno de todas las palabras de 16 bits en el paquete, excepto para el campo de autentificación. Si la longitud del paquete no es un numero entero de las palabras de 16 bits, el paquete es rellenado con un byte de cero antes de la suma de comprobación.
- AU type: Identifica el esquema de autentificación a ser usado por el paquete.
- Authentication: Campo de 64 bits para el esquema de autentificación.

Operación de OSPF

Los routers OSPF ejecutan una serie de pasos durante su activación y los repetirán en respuesta a los eventos de red, ejecuta estos pasos para cada red a la que esta conectado excepto para el calculo de la tabla de ruteo. Cada router mantiene una sola tabla de ruteo para todas las redes. Los pasos son:

1. Descubrimiento de vecinos OSPF.
2. Elección del DR (router designado).
3. Formación de adyacencias.
4. Sincronización de las bases de datos.
5. Calculo de la tabla de ruteo.
6. Anunciamiento de los estados de los enlaces.

Descubrimiento de vecinos.
Cuando se arranca un dispositivo el protocolo envía paquetes Hello a todos sus vecinos por todas sus líneas punto a punto y a todos los demás dispositivos de ruteo. Gracias a las respuestas que recibe sabe cuales son sus dispositivos de ruteo vecinos.
Determinación del DR
Mediante el protocolo Hello el router examina la lista de vecinos, desecha al que no tenga comunicación bidireccional, y graba el DR, el BDR (router designado de frontera) y la RP de cada uno.
El DR tiene las siguientes responsabilidades:

- El DR genera para la red los anuncios de los estados de los enlaces que inundan el área y describen esta red a todos los routers de todas las redes del área.
- El DR se hace adyacente a otros routers de la red. Estas adyacencias son centrales con respecto al proceso de inundación usado para asegurar que los anuncios alcanzan a todos los routers del área y que la base de datos topológica permanece igual.

El BDR tiene la responsabilidad de hacerse adyacente a los demás routers de la red. Lo que asegura que cuando ocupe el puesto del DR lo pueda hacer rápidamente.
Formación de adyacencias
OSPF se basa en el intercambio de información entre dispositivos de ruteo adyacentes que no es lo mismo que vecinos. Para que no todos los vecinos tengan que hablar con los demás se designa a uno como adyacente a todos los demás y es este el que intercambia información con los demás. Después de que se ha descubierto un vecino, asegurado la comunicación bidireccional y elegido un DR, se toma la decisión de si se deberá formar una adyacencia con uno de sus vecinos:

- En redes multiacceso, todos los routers se hacen adyacentes al DR y al BDR.
- En enlaces punto a punto cada router forma una adyacencia con el router del otro extremo.

Si no se quiere formar una adyacencia el estado de la comunicación con el vecino permanece en el estado de 2 vías.
Las adyacencias se establecen usando paquetes de descripción de base de datos que contienen un resumen de las bases de datos de estados de enlace del emisor.
Sincronización de las bases de datos
Después de terminar el proceso de intercambio de bases de datos cada router tiene una lista de aquellos anuncios para los que el vecino tiene mas instancias actualizadas que se solicitan por medio de paquetes LSR (Link State Request), como respuesta cada ruteador inunda la red con mensajes de actualización de estado de enlace Link State Update (LSU) indicando su propio estado y los costos de enlaces contenidos en su base de datos topológica, estos LSU contienen algunos o todos los anuncios solicitados, estos son confirmados mediante mensajes de confirmación de estado del enlace Link State Ack, si no se recibe respuesta se repite la solicitud. Los ruteadores envían mensajes cuando cambian los costos o cuado se cae o se levanta una línea. Los anuncios tienen cinco formatos de RLA (Route Link Advertisements).
Los mensajes Database Description informan todos los números de secuencia de las entradas disponibles en el emisor, permiten al receptor saber quien tiene la información mas reciente. Cualquier ruteador puede pedir información de estado de enlace a sus socios

emitiendo mensajes Link State Request. Cada par de ruteadores adyacentes verifica quien tiene la información mas reciente y la difunde en su área.
Cuando se ha respondido los paquetes LSR, las bases de datos se sincronizan y los routers se describen como totalmente adyacentes. La adyacencia se añade a los anuncios de los dos routers correspondientes.
Calculo de la tabla de ruteo
El router construye la tabla de ruteo con las bases de datos de estados de enlaces de las áreas con las que se conecta y ejecuta el algoritmo SPF. La tabla de ruteo que se construye siempre es cero, nunca se actualiza una tabla ya existente y la tabla mas vieja no se desecha hasta identificar los cambios entre las dos tablas. Los pasos para el cálculo de la tabla son:
1. El calculo de rutas intra-área se realiza construyendo el árbol mínimo para cada área conectada con el mismo router como raíz del árbol. Se checa si el área puede actuar como área de transito para enlaces virtuales.
2. Las rutas inter-área son calculadas checando los SLA (Link State Acknowledgment). Para los ABR solo se anuncian los mensajes correspondientes a la troncal.
3. Si el router se conecta a una o más áreas de transito, sustituye las rutas calculadas por rutas que pasen por áreas de transito si son mejores.
Las rutas externas son calculadas checando los anuncios externos del AS.
Cuando el algoritmo produce rutas de igual costo, OSPF puede balancear uniformemente la carga a través de ellas.
Anunciamiento de los estados de los enlaces.
Los routers anuncian periódicamente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del router que no esta activo, este suceso se detecta con un contador de inactividad, si no se resetea el contador se desbordará y el evento asociado sitúa el estado del vecino en down. La comunicación se debe restablecer desde cero, incluyendo la resincronización de las bases de datos. El ruteador también reenvía sus anuncios cuando su estado cambia. El ruteador lanza diversos anuncios para cada área por inundación. Los destinos se anuncian uno cada vez de tal forma que el cambio de una sola ruta puede inundar la red sin tener que enviar el resto de las rutas.
La operación se resume en la siguiente secuencia:

1. Por inundación cada ruteador informa a los otros ruteadores de su área sobre vecinos y costos.
2. Cada ruteador del área incluido el backbone construye el grafico para sus áreas calculando los caminos más cortos.
3. Los ruteadores de backbone reciben información de los ruteadores de borde de área para calcular la mejor ruta desde cada ruteador de backbone hacia todos los demás ruteadores
4. Los ruteadores de backbone propagan sus cálculos de mejores rutas hacia los ruteadores de borde de área.
5. Los ruteadores de borde de área propagan las mejores rutas dentro de sus áreas. Un ruteador puede así elegir la mejor ruta de salida hacia el backbone para enviar paquetes inter-área.

OSPF intercambia mensajes usando la dirección de multidifusión 224.0.0.5, el intercambio de información mediante LSAs se hace utilizando la dirección de multidifusión 224.0.0.6.
Las características del este protocolo son:

- Protocolo abierto, su algoritmo es publico no propietario.
- Tecnología de estado de enlaces.

- Para reducir el exceso de trafico realiza las actualizaciones de los cambios ocurridos, no de todas las rutas.
- Soporta tipos de servicio. Los administradores pueden instalar múltiples rutas hacia un destino dado, uno por cada tipo de servicio.
- Soporta diferentes métricas incluyendo distancia física y retardo
- Realiza un balanceo de cargas entre rutas de igual costo. Si el administrador especifica múltiples rutas hacia un destino con el mismo costo, OSPF distribuye el trafico entre todas las rutas de la misma forma.
- Partición en áreas. Permite que las redes y los hosts contiguos se agrupen juntos en áreas dentro de AS, simplificando la topología y reduciendo la cantidad de información de ruteo que se debe intercambiar. La topología de un área es desconocida para el resto de las áreas.
- Cada router mantiene un mapa topológico de la red entera.
- Propagación de modificaciones entre los enlaces.
- Los routers OSPF convergerán mucho más rápido que los routers RIP cuando hay cambios de topología gracias a las bases de datos de estados de enlaces sincronizadas.
- Se adapta automática y dinámicamente a los cambios.
- Localización automática de routers vecinos.
- Propagación de rutas aprendidas de fuentes externas. Permite el intercambio de información de ruteo externa, información de ruteo obtenida de otro AS.
- Soporta sistemas jerárquicos ya que con el crecimiento de la red se torno inviable para un ruteador conocer todas las rutas.
- Seguridad para evitar el engaño intencional con rutas falsas. Los intercambios entre routers se pueden autentificar mediante el uso de passwords.
- Routers designados en redes multiacceso.
- Utiliza métricas ponderadas para distintas velocidades del enlace. Un T1 podría tener una métrica de 1 y una LP a 9600 bps una de 10.
- A cada ruta se le asocia una mascara de subred, permitiendo subnetting de longitud variable (subredes) y supernetting (CIDR).
- OSPF soporta rutas especificas de hosts, redes y subredes.
- Minimiza los broadcast permitiendo una topología de grafo más compleja, el DR es el responsable de describir esa red a las demás redes del área.
- Permite configurar el ruteo dentro del AS según una topología virtual. Las áreas se pueden unir usando enlaces virtuales que crucen otras áreas sin requerir ruteo complicado.
- Permite el uso de enlaces punto a punto sin direcciones IP, lo que puede ahorrar recursos escasos en el espacio de direcciones IP.

- **Protocolo de ruteo interior RIPv2**

Es un protocolo de balance híbrido de naturaleza classful aunque también puede comportarse como classless. La métrica de RIPv2 es la misma de RIPv1, usa la cuenta de saltos.
RIPv2 es una extensión del protocolo RIPv1. La intención de RIPv2 es proporcionar una sustitución de RIP para redes pequeñas y medianas en presencia de subnetting variable (subredes) o supernetting (CIDR) y que pueda interoperar con RIPv1. Aprovecha que la mitad de los bytes de un mensaje RIP están reservados (deben ser cero) y que la especificación original estaba diseñada con las mejoras en la mente de los desarrolladores.
Modifica el formato de las RTE, Fig. 3.3.6.5, usa direcciones de multicast en vez de broadcast para realizar las actualizaciones. La dirección de multicast es la 224.0.0.9, puede responder a mensajes RIPv1 con mensajes RIPv1 a menos que se indique lo contrario.

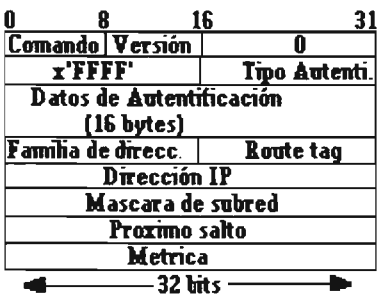


Fig. 3.3.6.5 Campos en RIPv2

Los campos de RIPv2 son:
- Command: se usa para especificar el propósito del datagrama.
- Versión: Este valor es 2. Le indica al router con RIPv1 que ignore los campos reservado, los que deben ser cero.
- Address family: Puede ser X'FFFF' solo en la primera entrada, indicando que se trata de una entrada de autentificación.
- Authentication type: Define como se han de usar los restantes 16 bytes. Los únicos tipos definidos son 0 indicando ninguna autentificación y 2 indicando que el campo contiene datos de password.
- Authentication Data: El password es de 16 bytes, texto ASCII plano, alineado a la izquierda y relleno de caracteres nulos ASCII (X'00').

Campos agregados en RTE:
- Route tag. Atributo que se debe preservar y propagar para esta ruta. Este campo informa acerca del origen de la información de encaminamiento. Se usa para separar rutas internas IGP de externas EGP y mejorar la interoperabilidad entre protocolos.
- Mascara de red: es la mascara de subred correspondiente a la subred destino.
- Próximo salto: Recomendación acerca del siguiente salto que el router debería usar para enviar datagramas a la subred o al host dado en la entrada. Es un aviso que permite optimizar si el IP es alcanzable por el receptor, sino se descarta.

La versión 2 de RIP tiene las siguientes mejoras respecto a la versión 1:
- Autentificación para la transmisión de información de RIP entre vecinos.
- Utilización de mascaras de red, con lo que a es posible utilizar VLSM.

- Utilización de mascaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de gestión MIB.

Además de estas mejoras, permite la redistribución de rutas externas aprendidas por otros protocolos de ruteo.
Algunas carencias que sigue teniendo son:

- Limitación en el tamaño máximo de la red ya que sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, por lo que no se puede usar en redes grandes.
- Continua presentando el problema de conteo al infinito si se presentan bucles, aunque se usen técnicas externas como el horizonte dividido con la inversa de poisson.
- Las métricas estáticas pueden ser cambiadas por el administrador de la red, pero no dan ninguna información del estado de la red.
- Solo permite al igual que la versión 1 una ruta por cada destino, con lo cual no se puede realizar balanceo de carga generando una pobre utilización de los enlaces.

La versión 2 al igual que la 1 genera muchísimo trafico al enviar toda la tabla de ruteo en cada actualización, con la carga de trafico que ello conlleva.
Para asegurar la interoperabilidad con RIP se tiene las siguientes restricciones para los routers RIPv2 que transmiten sobre una interfaz de red en la que un router RIP puede escuchar.

1. La información interna a una red nunca se debe anunciar a otra red.
2. La información acera de una subred mas especifica no se debe anunciar donde los routers vean una ruta de host.
3. Las rutas a superredes (rutas con una mascara de subred mas corta que la mascara natural de red) no se deben anunciar en los sitios en que puedan ser malinterpretados por routers RIP.

- **Protocolo de ruteo interior EIGRP**

Es un protocolo de balance híbrido de naturaleza classful aunque también puede comportarse como classless. La métrica de EIGRP es ancho de banda mas retardo.
El protocolo de ruteo de pasarela interior mejorado EIGRP (Enhanced Interior Gateway Routing Protocol) es una versión mejorada del IGRP de cisco. Es visto como un protocolo de pasarela interior (IGP), pero también ha sido visto extensivamente como un protocolo de pasarela exterior (EGP) para ruteo InterDominio. IGRP usa la tecnología de ruteo por vector distancia al igual que EIGRP. Las propiedades de convergencia y la eficiencia de operación de este protocolo han mejorado significativamente. El formato del encabezado EIGRP se observa en la Fig. 3.3.6.6

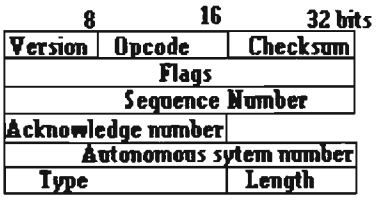


Fig. 3.3.6.6 Estructura del encabezado EIGRP

- Versión: La versión del protocolo.
- OPcode: 1. Actualización, 2. Reservado, 3. Consulta, 4. Hello, 5. IPX-SAP
- Type: 1. Parámetros EIGRP, 2. Reservado, 3. Secuencia, 4. Versión del software, 5. Siguiente secuencia multicast.
- Length: Longitud de la trama.

Protocolos de ruteo exterior

Los protocolos de ruteo exterior se usan para intercambiar información de ruteo entre distintos AS. Los mas usados son EGP y BGP, este ultimo prácticamente ha sustituido a EGP

- **EGP (Exterior Gateway Protocol)**

Es el protocolo usado por los gateways exteriores para intercambiar información de direccionamiento entre dominios de direccionamiento constituido por IGPs(Internal Gateway Protocol). Los gateways EGP solo pueden retransmitir información de accesibilidad ara las redes de su AS. Se usa para transportar información de alcance de la red entre gateways vecinos posiblemente en diferentes sistemas autónomos. Incluye mecanismos para adquirir información de vecinos supervisión de alcanzabilidad de vecinos e intercambio de alcanzabilidad de la red en la forma de mensajes de actualización. Se basa en el intercambio de mensajes de interrogación periódicos usando Hello/I heard you (IHU) para supervisar la alcanzabilidad del vecino y comandos de consulta para solicitar repuestas de actualización. Restringe los gateways exteriores al permitirles anunciar solo las redes de destino accesibles en el AS de la pasarela. Un gateway exterior que usa EGP pasa información a sus vecinos EGP pero no anuncia la información de accesibilidad de estos.
Se compone de tres partes:

- Soporta el protocolo Neighbor Adquisition Protocol (NAP) para establecer la comunicación. Consta de una solicitud y respuesta. Para que un gateway se convierta en vecino debe enviar un mensaje "Acquisition Confirm" como respuesta a un "Acquisition Request". Este paso es necesario para obtener información de ruteo de otro gateway.
- Soporta Neighbor Reachability Protocol. El gateway lo usa para mantener información en tiempo real sobre la accesibilidad de sus vecinos y determinar si la comunicación continua. Para este fin usa dos mensajes: el mensaje Hello y una respuesta de escucha.
- Soporta mensajes de actualización Neighbor Reachability Determination que llevan información de ruteo. Comprueba si el siguiente vecino es un camino valido para llegar a un destino particular.

El formato del mensaje es mostrado en la Fig. 3.3.6.7

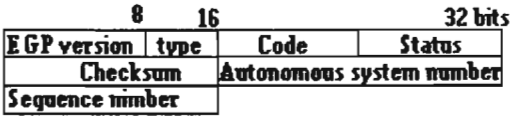


Fig. 3.3.6.7 Estructura del encabezado EGP

- EGP versión: El numero de versión.
- Type: Identifica el tipo de mensaje:

1. Indicación/respuesta de actualización.
2. Comando de petición.
3. Mensaje de adquisición de vecino.
4. Mensaje de alcance de mensaje.
5. Indicación/respuesta de error.

- Code: Identifica el código del mensaje.
- Status: Contiene información del estado dependiente del mensaje.
- Checksum: El complemento a uno de 16 bits de la suma del complemento a uno del mensaje EGP comenzando con el campo del numero de versión EGP, cuando se calcula el checksum, el campo en sí mismo debe ser cero.
- Numero de sistema autónomo: Numero asignado identificando el sistema autónomo particular.
- Numero de secuencia: Manda afirmación variable(comandos) o recibe afirmación variable (respuestas e indicaciones)

- **Protocolo BGP**

Existen 4 versiones de BGP (BGP-1, BGP-2, BGP-3 y BGP-4), la 1 y 2 ya están obsoletas mientras de las dos restantes la cuatro es la que actualmente tiene mas uso.
BGP-3 es un protocolo de ruteo inter-AS que se basa en la experiencia de EGP. A diferencia de otros protocolos de ruteo que se comunican mediante paquetes o datos, BGP-3 esta orientado a conexión, utiliza TCP como protocolo de transporte. Su numero de puerto bien conocido es el 179.
Cuando se establecen sistemas autónomos se crean dominios lógicos de administración en los que se tendrán políticas de ruteo independientes de los demás sistemas autónomos, cuando la administración de red requiere que dos o más sistemas autónomos se interconecten se tiene que hacer uso de los protocolos EGPs. Un protocolo EGP es utilizado cuando se quiere interconectar dos o más dominios lógicos de IGPs.
Los protocolos EGP tienen que ocuparse de los asuntos políticos. En particular el protocolo BGP se ha diseñado para permitir muchos tipos de políticas de enrutamiento aplicables al trafico inter AS.
Las políticas típicas comprenden consideraciones políticas de seguridad, o económicas. Estas se configuran manualmente en cada ruteador BGP, no son parte del protocolo mismo.
El protocolo EGP más utilizado es el BGPv4. BGP se encarga de mover los paquetes de una red a otra y de cuestiones relacionadas a las aplicaciones de políticas para restricción de trafico. Los principales cambios de esta versión respecto a sus antecesores se aplican al soporte de supernetting o CIDR, soporta prefijos IP y agregación de rutas. Debido a que

CIDR es radicalmente distinto de la arquitectura de ruteo normal de Internet, BGP-4 es incompatible con BGP-3. Por lo que BGP define un mecanismo para que dos BGPs negocien una versión que ambos entiendan, usando el mensaje OPEN.
La métrica que BGP utiliza son las rutas estáticas debido a que por políticas de los sistemas autonomos el habilitar ruteo dinámico no permitirá que los ruteadores realicen el intercambio de sus tablas de ruteo.
Los dispositivos de ruteo BGP se comunican entre sí estableciendo conexiones TCP. Este tipo de comunicación proporciona comunicación confiable y esconde todos los detalles de la red por la que pasa.
BGP es fundamentalmente un protocolo de vector distancia en el que cada dispositivo de ruteo mantienen el costo a cada destino y la trayectoria seguida. Estos valores son dados periódicamente a cada uno de los vecinos enviando mensajes. La esencia de BGP es el intercambio de información de ruteo entre dispositivos de ruteo. La información de ruteo actualizada se va propagando a través de un conjunto de redes. BGP involucra tres procedimientos funcionales que son:
- Adquisición de vecino: Dos dispositivos de ruteo son vecinos si están conectados a la misma subred y se han puesto de acuerdo en que ambos quieren intercambiar regularmente información de ruteo. Para llevar a cabo la función de adquisición de vecino un dispositivo de ruteo envía a otro un mensaje OPEN, si el dispositivo vecino acepta la solicitud, devuelve un mensaje KEEPALIVE como respuesta.
- Detección de vecino inalcanzable: Para mantener la relación de vecino establecida se realiza la detección de vecino alcanzable enviándose periodicamente mensajes KEEPALIVE.
  - Detección de red alcanzable: Para la detección de red alcanzable es necesario que cada dispositivo de ruteo tenga una base de datos con todas las redes que puede alcanzar y la mejor ruta para alcanzarlas. Cuando se realiza un cambio en la base de datos es necesario enviar un mensaje Update por difusión a todos los dispositivos de ruteo que implementan BGP para que puedan acumular y mantener la información necesaria.

El protocolo BGP es un protocolo de ruteo de intersistemas autónomos. Un sistema autónomo puede contener múltiples dominios de direccionamiento, cada uno con su propio protocolo interno de sistema autónomo, o IGP. Dentro de cada sistema autónomo pueden haber varios gateways que se pueden comunicar con los gateways de otros sistemas. Un sistema autónomo aparece ante otro sistema autónomo como un direccionador consistente. La función primaria de un sistema hablando BGP es intercambiar información de alcance de la red con otros sistemas BGP. BGP-4 proporciona un nuevo conjunto de mecanismos para soportar ruteo interdominio classless (CIDR Classless Interdomain Routing). Su formato se muestra en la Fig. 3.3.6.8.

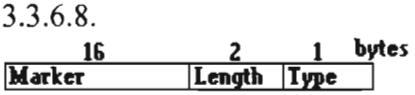


Fig. 3.3.6.8 Estructura del encabezado BGP-4

- Marker: Un mensaje de 16 bytes que contiene un valor predecible por el receptor del mensaje.
- Length: La longitud del mensaje incluido el encabezado.
- Type: Tipo de mensaje: Open, Update, Notification, keepalive.

Algunos cambios de BGP-4 respecto a sus antecesores son:

- El numero de versión en la cabecera es 4.
- CIDR elimina el concepto de clase de red del ruteo inter-dominio, sustituyéndolo por el de prefijo IP.
- La lista de redes en un mensaje Update por la información de alcanzabilidad de la capa de red NLRI.
- Introduce la agregación de múltiples rutas de AS en entradas únicas o agregadas. El uso de agregados puede reducir dramáticamente la cantidad de información de ruteo requerida.
- BGP-4 modela conceptualmente los datos de un sistema que ejecuta BGP en tres series de RIBs (bases de información de ruteo): uno para los datos obtenidos de vecinos BGP, otro para datos locales obtenidos de las operaciones de las políticas de ruteo locales y uno para datos que han de ser anunciados en mensajes UPDATE.
- Permite la negociación del valor Hold-Time por cada conexión de modo que los extremos de la misma usen el mismo valor.

La tabla 3.3.6.1 resume algunas características de los protocolos de ruteo.

Protocolo	Algoritmo	Método	Métrica	Convergencia	D.A.	Escalabilidad
Protocolos de ruteo Interior						
Protocolos que usan el método de vector distancia						
RIPv1	Bellman Ford	Classful	Hops ≤15	Broadcast de la tabla entera cada 30 seg.	120	Baja
IGRP	Bellman Ford	Classful	BW+ delay	Broadcast de la tabla entera cada 30 seg.	100	Media
Protocolos que usan el método de estado de enlace						
OSPF	Dijkstra	Classless	Costo	Multicast de la tabla parcial cada 30 seg.	110	Alta
IS-IS		Classless			115	Alta
Protocolos de balance hybrido						
RIPv2	Bellman ford	Classful y classless	Hops ≤ 15	Broadcast de la tabla entera cada 30 seg.	125	Baja
EIGRP	Dual Difussion Update Algorithm	Classful y classless	BW+ delay	Multicast de la tabla parcial cada 120 min.	90	alta
Protocolos de ruteo exterior						
BGP y BGPv4						Alta
IDRP						

Tabla 3.3.6.1 Protocolos de ruteo.

Donde:

- DA=Distancia administrativa.
- Hops=Cuenta de saltos.
- BW=Ancho de banda.
- Delay=retardo del enlace.

3.3.7 Servicios y aplicaciones

Los diferentes servicios a los que se puede tener acceso en Internet (recordar que Internet esta basado en IP) vienen dados por los protocolos que pertenecen al nivel de aplicación y que forman parte del stack TCP/IP.
Por tanto podríamos decir de forma indirecta que los servicios que puede proporcionar IP en realidad son los mismos de TCP/IP ya que debemos recordar que todos los protocolos de aplicación y de transporte de la pila TCP/IP corren sobre IP por lo tanto, los servicios de IP pueden ser:
Servicios de ejecución remota, transferencia de datos, correo electrónico, conexión remota, Impresión, diagnostico, resolución de nombres, Configuración dinámica, ruteo, seguridad, proxy, gestión.
El servicio mas ampliamente utilizado actualmente es el acceso a Internet. Hablar de Internet es hablar del protocolo IP. Internet de ser una red de investigación y uso militar se convirtió en una autopista de información para transmitir imágenes en movimiento, dibujos, sonidos, voz y una gran cantidad de datos.
El acceso a Internet es proporcionado por cualquier proveedor que disponga de esta posibilidad para lo cual se hace completamente necesario el protocolo TCP/IP. El numero IP que dispondrá como dirección la estación del usuario es suministrada por el proveedor y será una dirección valida de Internet. Algunos servicios o aplicaciones que ofrece Internet son:

- Acceso a cualquier tipo de información.
- Conexión mundial por voz, video y datos.
- Comercio electrónico.
- Conexión con todo tipo de ordenadores.
- Movimientos financieros.
- Newsgroup.
- Servicios de teledistancia:
  - e-mail.
  - WebChat.
  - Web hosting.
  - Transferencia de archivos.
  - Videoconferencias.
  - Noticias.
- Sistema de dominios.
- Sistema de distribución de información por medio de la WWW.
- Gopher.
- FTP.

- Telnet.
- Servicios multimedia.
- Conferencias telefónicas.
- Tarificación.
- Administración de la red.
- Comercio.
- Multicanales de televisión.
- Internet rápido.

El protocolo IP permite la implementación y comunicación de

- Intranets.
- Extranets.
- VPN (Virtual Private Networks).

Algunas aplicaciones mas especificas basadas en IP son:

- VoIP.
- IPoATM.
- Telefonía IP.
- IPoDSL.

3.4 IPv6

Uno de los principales motivos para definir una nueva versión del protocolo IP fue la limitación impuesta por el campo de direcciones en IPv4, así como la ineficiente división en las clases A, B, C y D. Las técnicas implementadas para tratar de aminorar los problemas mencionados anteriormente, a largo plazo ya no tendrán la capacidad de seguir manteniendo el sistema actual debido a la aparición de sistemas móviles para datos como GPRS y UMTS que requieren un amplio espectro de direcciones IP, este requerimiento difícilmente podría ser cubierto por la estructura de direcciones IPv4.
De esta forma algunas razones que hacen necesario el uso de un nuevo protocolo de Internet son:

- Mejorar las limitaciones del protocolo IPv4 como el uso de NAT (no permite el despliegue de nuevas aplicaciones y servicios comprometiendo el desempeño, robustez y seguridad de Internet a la vez que impide el uso de servicios en dispositivos que son llamados por otros como teléfonos-IP, además del costo que implica el overhead por su uso) agregando nuevas mejoras como la seguridad, calidad de servicio y autoconfiguración.
- Tener un protocolo que se adapte a las nuevas necesidades del Internet actual y que permita el desarrollo de las nuevas aplicaciones.
- Contar con mas direcciones para millones de nuevos dispositivos (celulares con capacidad de acceso a Internet, electrodomésticos, PDAs, automóviles), para millones de usuarios necesitados de contar con conexión a Internet y que con IPv4 están restringidos, para el despliegue de nuevas tecnologías que estén siempre conectadas (always-on) como xDLS, cable, ethernet, para nuevas aplicaciones y servicios que requieren direcciones IP únicas.
- La adopción de IPv6 permitirá regresar al uso y explotación del modelo original de Internet con las ventajas que se obtienen de tener una comunicación de extremo a extremo, sin cajas negras de por medio.

3.4.1 Características de IPv6

IPv6 conserva la mayor parte de las características y conceptos de operación de IPv4, pero agrega nuevas capacidades y funcionalidades que permiten flexibilizar y modelar nuevos conceptos de operación. En primer instancia resuelve el tema de numero de direcciones IP.
La versión 6 de IP tiene muchos nuevos cambios respecto a la versión que se usa actualmente, esos cambios caracterizan a IPv6. Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 los 128 bits, eliminando todas las restricciones del sistema actual. Otros de los aspectos mejorados son la seguridad y la calidad de servicio, que en la versión anterior eran uno de los mayores problemas. Además el nuevo formato de la cabecera se ha organizado de una manera más optimizada para su proceso más eficiente por parte de los ruteadores, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.
Algunas de las características que posee IPv6 comparado con IPv4 son las siguientes:

- Longitud de direcciones. La característica más sobresaliente de IPv6 es el número de bits usados para la representación de las direcciones IPv6, en IPv4 tenemos que

las direcciones son de 32 bits, en IPv6 las direcciones son de 128 bits, es decir son cuatro veces más grandes

- Direcciones con alcance y escalabilidad global. La gran capacidad de direccionamiento de IPv6 es consecuencia del numero de bits que utiliza, en IPv4 tenemos 2^{32} que son aproximadamente 6 billones de direcciones en total, en IPv6 tenemos 2^{128} que equivalen en el peor caso aproximadamente a 1564 direcciones por metro cuadrado.
- Posibilidades extendidas de direccionamiento y de ruteo. Al aumentar el tamaño de la dirección IP de 32 a 128 bits soportan muchos mas nodos direccionables, mas niveles de direcciones jerárquicas y una autoconfiguración más sencilla de las direcciones, asimismo pueden tener cabida dispositivos que en un futuro quieran tener conexión a la red como los televisores. Se definen un mecanismo adaptable de difusión y un nuevo tipo de direcciones en cluster.
- IPv6 usa el termino paquete mas que datagrama, pero el significado es el mismo, aunque los formatos sean los distintos.
- Los paquetes tienen la posibilidad de tener una carga útil (payload) de datos de mas de 65535 bytes.
- IPv6 introduce un nuevo termino, nodo, para un sistema que ejecuta IPv6, es decir, un nodo es un host o un router. Un host IPv6 es un nodo que no envía paquetes IPv6 que no están dirigidos explícitamente a el. Un router al igual que en IPv4 es un nodo que envía paquetes no dirigidos explícitamente a el.
- En IPv6 se tiene una arquitectura de red jerárquica para un ruteo eficiente
- Agilización del ruteo. IPv6 maneja datagramas IP eficientes y extensibles mediante un formato de cabecera simplificado. El encabezado del paquete aumenta de 20 bytes en IPv4 a 40 bytes en IPv6, el cual aunque se duplica tiene muchas ventajas como la eliminación de campos redundantes, los campos de dirección tienen tamaño fijo y se alinean en palabras de 32 bits lo que contribuye a una eficiencia en el procesamiento de paquetes. Algunos campos del formato de la cabecera han sido suprimidos o convertidos en opciones y la cabecera es simplificada y reducida a un tratamiento común en todos los ruteadores, lo que disminuye el costo del tratamiento en los mismos.
- Posibilidades de extensión de las cabeceras y de las opciones. En IPv6 las opciones están contenidas en cabeceras suplementarias colocadas entre la cabecera IPv6 y la cabecera del paquete de transporte (T-PDU Transport Protocol Data Unit). La mayoría de las opciones de las cabeceras de IPng no son examinadas ni tratadas por los ruteadores intermedios. Esto simplifica y acelera el procesamiento que realiza un dispositivo de ruteo sobre los datagramas IPv6 en comparación a los datagramas IPv4 a la vez que es más fácil incorporar opciones adicionales. A diferencia de IPv4 las opciones pueden ser de longitud variable, no existiendo un tamaño límite. Una característica de IPv6 es la posibilidad de codificar en las opciones la acción que un ruteador o una estación de trabajo tiene que realizar si la opción es desconocida, esto agrega funcionalidad suplementaria a la red operativa con un mínimo de modificaciones.
- IPv6 elimina el control de errores en la cabecera.
- IPv6 elimina la fragmentación en los ruteadores. Realiza la fragmentación solo en la fuente ya que los paquetes IP son eficientes y extensibles sin que haya necesidad de

realizar la fragmentación en los routers pues son alineados a 64 bits con su cabecera de longitud fija más simple que agiliza su procesado por parte del router.

- Calidad de servicio. Mejora la calidad de los servicios y asignación de recursos ya que provee capacidades para administrar flujos de datagramas relativos a servicios particulares, los cuales pueden recibir un tratamiento preferencial lo que garantiza un nivel de comunicación para estos servicios, para esto IPv6 presenta la capacidad de etiquetas de flujo, esta capacidad es usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de trafico particular que requieren manejo especial por los routers IPv6, como los servicios de comunicación de audio y video en tiempo real (videoconferencia o la voz).
- Seguridad. IPv6 Posee seguridad integrada con la implementación de IPsec obligatoria por lo que proporciona capacidades de seguridad mediante el uso de las posibilidades de autentificación y confidencialidad. IPv6 define extensiones que permiten la autentificación de los usuarios y la integridad de los datos mediante herramientas de criptografía. El soporte de IPsec es un requerimiento del protocolo IPv6 para tener seguridad desde el núcleo del protocolo.
- Autoconfiguración de direcciones. IPv6 contiene varias formas de autoconfiguración como la configuración Plug and Play, la autoconfiguración de direcciones de nodos sobre una red aislada gracias a las características de DHCP. Esta característica proporciona una asignación dinámica de direcciones IPv6. La autoconfiguración de direcciones es simple en direcciones tipo Aggregatable Global Unicast donde los 64 bits superiores son establecidos por un mensaje desde el router y los 64 bits más bajos son establecidos por la dirección MAC (en formato EUI-64). De esta forma el largo del prefijo de la subred es de 64 por lo que la mascara de red ya no implica preocupación alguna. Asimismo el largo del prefijo no depende del numero de hosts por lo que la asignación es más simple. Esta característica de autoconfiguración también permite que la renumeración en caso de cambiar de operador de Internet sea más fácil.
- Multihoming. Presenta características de renumeración y multihoming que facilitan el cambio de proveedor de servicios.
- Movilidad. Características de movilidad, con lo cual un nodo tiene la posibilidad de mantener la misma dirección IP, a pesar de su movilidad. Proporciona soporte mejorado para dispositivos de computo móviles e IP móvil.
- Mayor numero de direcciones multicast.
- Mayor flexibilidad de direccionamiento ya que incluye el concepto de dirección de monodistribución o envío a uno (anycast), este concepto permite entregar un paquete solamente a un nodo seleccionado entre un conjunto de nodos.
- Ruteo. El ruteo es más eficiente en el backbone de la red, gracias a la jerarquía de direccionamiento basada en la agregación.
- Soporta protocolos de ruteo ampliamente instalados.
- Posibilidades para el source route. IPv6 tiene una función extendida de Source Routing gracias a SRDP (Source Route Demanding Protocol) para difundir el ruteo a rutas interdominio e intradominio.
- Con IPv6 ya no se necesita hacer uso de NAT (Network Address Translation) y ALG (Application Layered Gateway).

Las características de IPv6 representan muchos cambios a IP, estos cambios mejoran a IPv4 en muchos sentidos, el direccionamiento expandido de IPv6 significa que IP puede seguir creciendo sin preocuparse del agotamiento de recursos. La arquitectura de direccionamiento ayuda a mejorar la situación para un ruteo más eficiente, ya que el formato del encabezado simplificado mejora la eficiencia de ruteo al requerir menos procesamiento de los routers, mientras las mejoras en las extensiones y opciones significan que necesidades especiales pueden ser cumplidas sin afectar significativamente el desempeño tanto de paquetes normales como paquetes de necesidades especiales. El etiquetamiento de flujo proporciona otro mecanismo para tratar flujos de paquetes eficientemente, siendo particularmente útil para aplicaciones de tiempo real. Las mejoras en la autentificación y privacidad hacen a IPv6 un protocolo más deseable para usos comerciales que requieren tratamiento de información sensible o recursos.

3.4.2 Formato de los paquetes IPv6

IPv6 incrementa la longitud de la cabecera IP de 20 a 40 bytes. La cabecera IPv6 contiene dos direcciones de 16 bytes (fuente y destino) precedidas de 6 bytes de control, por su parte la cabecera IPv4 tiene dos direcciones de 4 bytes precedidas de 12 bytes de control y seguidas de algunas opciones.
Aunque las direcciones IPv6 son cuatro veces más grandes que en IPv4, la cabecera es solo dos veces mayor que la cabecera IPv4.
El formato de la unidad de datos de protocolo (PDU) de IPv6, datagrama o paquete tiene el formato general de la Fig. 3.4.2.1

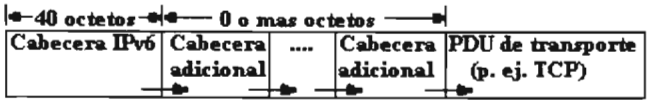


Fig. 3.4.2.1 Formato de la PDU de IPv6.

En el formato de la unidad de datos de protocolo (PDU) del datagrama (paquete), el tamaño de la cabecera obligatoria que el protocolo IPv6 agrega a los datos es de 320 bits o 40 bytes (en la versión 4 el tamaño mínimo de la cabecera es de 20 bytes), sin embargo la nueva cabecera, Fig. 3.4.2.2, se ha simplificado con respecto a la de IPv4.

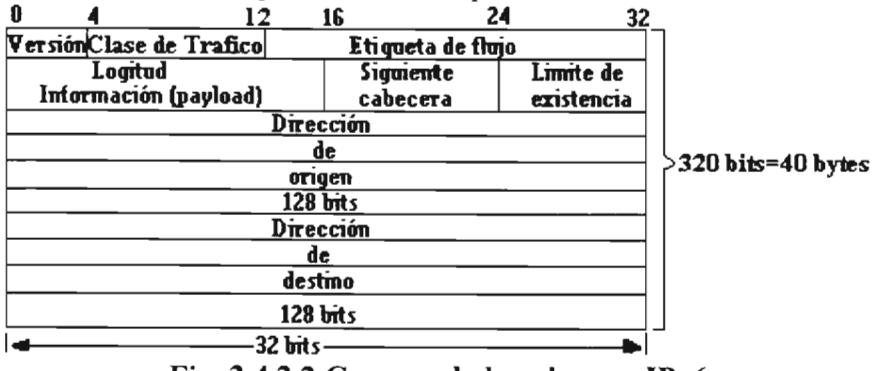


Fig. 3.4.2.2 Campos de la cabecera IPv6

Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. La cabecera IPv6 tiene 8 campos frente a los 12 campos de la cabecera IPv4. La reducción de la información de control y la eliminación de opciones de la cabecera tienen como fin optimizar el procesamiento del paquete y esta basada en que muchos de esos campos realizan funciones redundantes. Los campos de uso poco frecuente que se han eliminado de la cabecera se han pasado a extensiones de cabecera opcionales. De esta manera los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar el rendimiento en la transmisión.
El encabezado puede ser simplificado como resultado de algunos cambios en la forma en que IP trabaja. Por una parte hacer a todos los encabezados de la misma longitud elimina la necesidad del campo longitud del encabezado. Por otro lado, al cambiar las reglas acerca de la fragmentación, algunos campos pueden ser removidos del encabezado. Finalmente eliminando la comprobación (checksum) del encabezado, no afectaría a la confiabilidad en ninguna forma debido a que las comprobaciones son ejecutadas por protocolos de niveles superiores (TCP y UDP).
Los campos del formato completo de la cabecera sin las extensiones son los siguientes:

- **Versión (Version):**

Campo que indica el número de versión del protocolo IP, en este caso tendrá el valor 6. El tamaño de este campo es de 4 bits. Este campo es igual en tamaño al de IPv4 que contiene el numero 4. El uso de este campo es limitado ya que los paquetes IPv4 e IPv6 no se distinguen sobre la base del valor contenido en el, sino en función de un tipo de protocolo diferente (0800H-IPv4, 86DDH-IPv6) en el encapsulamiento de capa 2 (como en Ethernet o PPP).

- **Clase de trafico CoT (Class of Traffic) o prioridad (Priority):**

Este campo normalmente se usa muy estrechamente con el de etiqueta de flujo, habilita al nodo fuente a diferenciar paquetes que el entrega asociándoles diferentes prioridades de entrega frente a otros provenientes de la misma fuente, su formato es el de la Fig.3.4.2.3

Fig. 3.4.2.3

Donde:

- x: Es un bit bandera que indica si el trafico tiene control de flujo. Si esta activo, no hay control de flujo (no hay realimentación desde los receptores), si no esta activo, existe un control de flujo.
- Class: Es un numero de tres bits que indica el tipo de trafico. Contiene el valor de la prioridad de entrega, clase de trafico o importancia del paquete que se esta enviando con respecto a otros paquetes provenientes de la misma fuente, con este campo el paquete se clasifica como un paquete para proporcionar control de congestión o no, en base a 16 valores de prioridad. Los valores de la prioridad están divididos en rangos de comportamiento de la red: trafico donde la fuente proporciona control de congestión y trafico sin control de congestión. Para cada clasificación hay 8 niveles de prioridad. De esta forma primeramente los paquetes se clasifican como pertenecientes ya sea a trafico para el que la fuente proporciona control de congestión o bien trafico para el que no hay control de congestión, posteriormente a los paquetes se les asigna uno de los ocho niveles de prioridad de la clasificación

donde se encuentren. Este campo es parte del complemento relacionado con calidad de servicio (QoS) no provisto en IPv4. La longitud del campo es de 4 bits u 8.

El protocolo usado para controlar el flujo puede redefinir los valores, algunos valores recomendados para el trafico con control de flujo son mostrados en la tabla 3.4.2.1:

	Valor	Trafico con control de congestión
Prioridad creciente	0	Trafico sin caracterizar
	1	Trafico de relleno (filler) como netnews
	2	Transferencia de datos no esperada como e-mail
	3	Reservado
	4	Transferencia de gran cantidad de datos esperada (FTP, HTTP)
	5	Reservado
	6	Trafico interactivo, como Telnet, X-Windows
	7	Trafico de control de Internet, como protocolos de ruteo, SNMP

Tabla 3.4.2.1 Niveles de prioridad para la clasificación de trafico con control de congestión.

Los valores de 0 a 7 son usados para especificar la prioridad del trafico para el cual la fuente proporciona control de flujo (trafico).

El trafico con control de congestión es el trafico al que el origen realiza una reducción del envío en respuesta a la congestión como es el caso de TCP que al no recibir la confirmación de recepción de los segmentos debido a la congestión reenviara el segmento y reducirá el flujo de segmentos (tamaños variables de ventanas). El trafico con control de congestión es aceptable cuando se permite un retardo variable en la transmisión de paquetes e incluso que lleguen fuera de orden.

Aplicaciones en particular; Trafico grande (netnews...), interactivo (telnet...), o trafico de control de Internet (SNMP, routing protocol...).

Este campo también es conocido como Diffser (Servicios Diferenciados) o Traffic Class (Clase de trafico), el cual es heredero del campo ToS Type of Service (Tipo de servicio) de IPv4.

8-15: Usado para marcar paquetes no afectados por el control de flujo, como por ejemplo paquetes de tiempo real enviados sin control de retorno por parte de los receptores.

Los valores 8 a 15 son usados para el trafico sin control de congestión (paquetes de tiempo real enviados sin control de retorno o respuesta por parte de los receptores a la congestión) como muestra la tabla 3.4.2.2

	Valor	Trafico sin control de congestión
Prioridad creciente	8	Mas dispuesto a ser descartado como video de alta fidelidad
		. . . . .
	15	Menos dispuesto a ser descartado como audio de baja calidad

Tabla 3.4.2.2 Niveles de prioridad para la clasificación de trafico sin control de congestión.

El trafico sin control de congestión es el que requiere una velocidad de transferencia y retardo de entrega constantes y en el que no tiene sentido una retransmisión de paquetes descartados. Sus prioridades van desde la mas alta (8, paquetes que la red descartara primero bajo condiciones de congestión) a la mas baja (15, paquetes que se descartaran al final, si es absolutamente necesario). Un ejemplo de este tipo de trafico son los paquetes en tiempo real producidos por la transmisión de películas o sonido.
Aplicaciones en general. Para aquellos paquetes que el emisor desea que se descarten en condiciones de congestión (por ejemplo trafico de video de alta o baja fidelidad).
Para trafico sin control de flujo, el valor de Class se usa como prioridad cuando hay algún problema. Cuanto más baja sea la prioridad el emisor no se debe preocupar de que el paquete llegue a su destino.

- **Etiqueta de flujo (Flow Label):**

Campo de 24 bits usado por una fuente para etiquetar un conjunto de paquetes pertenecientes al mismo flujo, cada paquete requiere un tratamiento en tiempo real especial (calidad de servicio no por default, servicio en tiempo real) por parte de los routers que lo soporten.
IPv6 define el flujo como una secuencia de paquetes en alguna forma correlacionada (generados por la misma aplicación), enviados desde un origen particular a un destino particular (unicast o multicast), para los cuales el emisor desea un trato especial y que comparten parámetros (como la dirección fuente, destino, QoS, autorizaciones, autenticación, seguridad) este flujo es unívocamente identificado por la combinación de la dirección fuente y una etiqueta de flujo diferente de cero. Pueden existir varios flujos entre la fuente y el destino (misma dirección fuente pero etiquetas de flujo diferentes), así como también trafico que no esta asociado con ningún flujo (etiqueta de flujo igual a cero). Los flujos pueden ser unicast (de un nodo a otro nodo) o multicast (de un nodo a un conjunto de nodos).
Este campo también es parte del complemento relacionado con QoS. El valor de este campo es un numero único pseudo aleatorio (1 a FFFFFF) que el nodo fuente asigna a un flujo. La aleatoriedad es necesaria para permitir a los routers emplear una secuencia de bits del flujo como clave de dispersión (hash), el valor debe ser diferente de las etiquetas de flujo en uso o de las recientemente usadas. El flujo es identificado unívocamente por la combinación de una dirección fuente y una etiqueta de flujo de 24 bits diferente de cero, todos los paquetes que van a formar parte del mismo flujo tienen asignada por el origen la misma dirección origen, dirección destino, prioridad y etiqueta de flujo. La forma de manejar los paquetes pertenecientes a un flujo dado puede ser especificado con información dentro de los paquetes (opciones adicionales a los datagramas) o con un protocolo separado como RSVP (Resource Reservation Protocol).
Si cualquiera de los encabezados de extensión Hop-by-Hop o Routing están presentes deben ser los mismos en todos los paquetes pertenecientes al mismo flujo.
Para el origen un flujo es una secuencia de paquetes que son generados por una única aplicación en el origen y tienen los mismos requisitos del servicio de transferencia.
Para los ruteadores, el flujo es una secuencia de paquetes que comparten atributos para ser tratados por los ruteadores. Puede haber diferentes atributos como: de ruta, de asignación de recursos, de requisitos relativos al descarte, contabilidad de paquetes transmitidos y de seguridad. Los paquetes que pertenecen al mismo flujo deben ser tratados coherentemente por los ruteadores. El ruteador puede tratar los paquetes de diferente forma incluyendo la

asignación de diferentes tamaños de memoria temporal, otorgándole diferente precedencia en términos de reenvío o solicitando de las subredes diferentes calidades de servicio.
Para evitar el tener paquetes de cabeceras muy grandes en IPv6 los requerimientos de flujo se definen antes de comenzar el flujo mediante la etiqueta única de flujo. En este caso el dispositivo de ruteo debe guardar la información sobre los requisitos de flujo de cada flujo, así cada vez que le llega un paquete solo tiene que analizar las etiquetas de flujo para determinar las acciones que debe realizar. De esta forma cuando los routers reciben el primer paquete de un nuevo flujo procesan la información transportada por el encabezado IPv6 y por los encabezados de extensión recuerdan el resultado (tiempo de vida =6 segundos) en una memoria cache y después aplican el mismo resultado a los demás paquetes del mismo flujo leyéndolo directamente de la memoria cache.
Los nodos que no puedan soportar la función del campo etiqueta de flujo deben ponerlo a cero cuando originen un paquete, pasarlo sin cambio cuando reenvíen un paquete o ignorarlo cuando lo reciban.
Estos dos últimos campos (Priority y Flow Label) son la base para la implantación de calidad de servicio (QoS) al trafico IPv6 mediante el control de flujo y asignación de prioridades, lo cual es indispensable para la implantación de IPv6 en redes multiservicio que manejan voz, datos y video.

- **Longitud de la información útil (Payload length):**

Es la longitud en bytes de los datos (extensión headers incluyendo la PDU del nivel de transporte) que se encuentran a continuación de la cabecera. Tiene un tamaño de 16 bits por lo que la información útil del paquete puede ser de hasta 65536 bytes. Si la longitud de la carga útil es mayor de 64 kb, este campo vale 0, lo que indica la presencia de la cabecera extensión Jumbo Payload la cual da la verdadera longitud. Este campo seria como una modificación del campo longitud total del encabezado IPv4.

- **Siguiente cabecera (Next Header):**

Campo de 8 bits que identifica el tipo de encabezado que se sitúa a continuación de la actual del encabezado IPv6 y antes del campo de datos (payload) del datagrama IPv6. El valor de este campo es el mismo que el del protocolo en la versión 4 de IP. Los dos Next Headers más comunes son TCP (6) y UDP 17). También indica la presencia de cabeceras de extensión que proporcionan los mecanismos para añadir información opcional al paquete. Los encabezados de extensión poseen un numero de encabezado según la siguiente lista:
00 = Extensión de encabezado Opciones Salto-por-salto.
41 = Extensión de encabezado IPv6.
43 = Extensión de encabezado para fragmentación.
51 = Extensión de encabezado para autenticación AH.
60 = Extensión de encabezado opciones de destino.
50 = Extensión de encabezado para el encapsulamiento de seguridad de la carga útil ESP.
xx = Encabezado de capas superiores. El valor xx depende de los números de protocolos de capas superiores asignados.
58 = Protocolo de mensajes de control de Internet ICMP.
59 = No hay siguiente encabezado.
La tabla 3.4.2.3, nos muestra un listado mas detallado de números de encabezado:

Valor de Next Header	Identificación	Protocolo
0		Reservado (IPv4)
0	HBH	Hop-by-Hop (IPv6)
1	ICMP	Internet Control Message (IPv4)
2	IGMP	Internet Group Management IPv4)
3	GGP	Gateway to Gateway Protocol
4	IP	IP en IP (encapsulación IPv4)
5	ST	Stream
6	TCP	Transmission Control
8	EGP	Exterior Gateway Protocol
9	IGP	Cualquier protocolo de ruteo intradominio
17	UDP	User datagram
29	ISO-TP4	ISO Transport Protocol class 4
41	EH	Extension Header (IPv6)
43	RH	Routing Header (IPv6)
44	FH	Fragmentation Header (IPv6)
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Reservation Protocol
50	ESP	Encapsulation Security Payload (IPv6)
51	AH	Authentication Header (IPv6)
54	NHRP	NBMA Next Hop Resolution Protocol
58	ICMPv6	Internet Control Message (IPv6)
59	Null	No next header (IPv6)
60	DOH	Destination Options Header (IPv6)
80	ISO-IP	ISO Internet Protocol (CLNP)
88	IGRP	IGRP
89	OSPF	Open Shortest Path First

Tabla 3.4.2.3 Valores del campo Next Header.

Con este campo IPv6 puede encapsular diferentes tipos de paquetes, estos encabezados o protocolos encadenados a menos que se especifique solamente serán procesados por el nodo o nodos destino, lo que hace eficiente el trabajo de los ruteadores al no tener que procesar las opciones de cada paquete en cada salto.

- **Limite de existencia (Hop limit):**

Campo es de 8 bits que tiene el mismo propósito que el campo TTL (Time to live) de la versión 4 pero ahora se mide en saltos y no en segundos, dos fueron las razones para cambiar la medición a saltos:

- IP envía normalmente los datagramas a mas de un salto por segundo y el campo TTL se decrementa siempre en cada salto, así para efectos prácticos se mide en saltos y no en segundos.
- Algunas implementaciones de IP no causan la expiración de los datagramas en base al tiempo transcurrido.

Este valor disminuye en una unidad cada vez que el paquete pasa por un nodo (típicamente un router) que lo retransmite. El paquete es descartado si su hop limit es decrementado a cero. La función principal de este campo es identificar y descartar paquetes que están

atrapados en un circulo (looping) debido a información de ruteo errónea, ya que entre dos nodos no puede haber mas de 255 saltos (enlaces), es decir no hay mas de 254 routers.

- **Dirección de origen (Source address):**

Campo de 128 bits que contiene la dirección del host que envía el paquete. Su longitud es 4 veces mayor que en la versión 4.

- **Dirección destino (Destination address):**

Campo de 128 bits que contiene la dirección del receptor del paquete, aunque puede no coincidir con la dirección del host final si esta presente la cabecera de ruteo. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP.

3.4.3 Cabeceras adicionales de IPv6

A diferencia de IPv4 (agrega opciones al final del encabezado IP, estas opciones a menudo no son usadas y sin embargo deterioran el desempeño del router por que tienen que ser checadas en cada paquete), IPv6 agrega opciones en encabezados de extensión separados. En esta forma el encabezado opcional solamente necesita ser examinado y procesado conforme sea necesario.

Las opciones de IPv6 son puestas en encabezados separados (Extensión Headers-EH) que se sitúan después de la cabecera normal y antes de la cabecera que incluye el protocolo de nivel de transporte, Fig. 3.4.3.1. Estos EH se cuentan como parte de la carga efectiva de la trama. Los datos situados en cabeceras opcionales se procesan solo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento, ya que salvo excepciones apenas son examinadas o manipuladas por los nodos. La única excepción es la cabecera nodo por nodo (Hop-by-Hop) que lleva información que deberá ser examinada por los nodos de la red, esta cabecera tiene que estar inmediatamente después de la cabecera IPv6.

Cambios en la forma en que las opciones del encabezado IP son codificadas, permiten un reenvío más eficiente, una flexibilidad mayor para introducir nuevas opciones en el futuro, limites menos rigurosos en la longitud de las opciones ya que la cabecera no esta limitada a un valor fijo de bytes como ocurría en la versión 4.

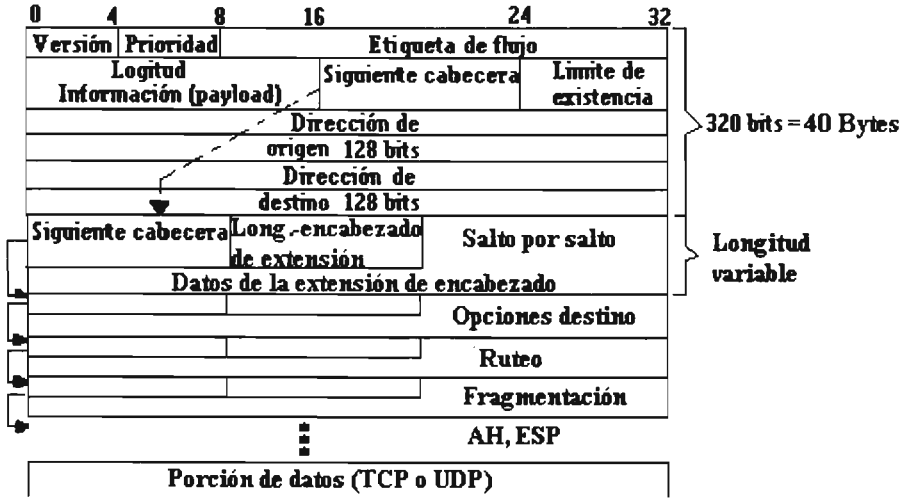


Fig. 3.4.3.1 Encabezado extensión IPv6.

Cada paquete IPv6 puede contener cero, una o más cabeceras adicionales.
Por razones de eficiencia las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes (64 bits) para conservar una alineación.
En un paquete IPv6 además de la cabecera principal de IPv6 existen algunas opciones o cabeceras adicionales, cada una de ellas tiene asignado un valor distinto para ser identificada en el campo próxima cabecera. Cada cabecera tiene un campo de 8 bits, Next Header (campo para encadenar encabezados), que identifica el tipo de la cabecera siguiente, este campo es el primer byte de cada cabecera.
Un paquete IPv6 puede no tener encabezado de extensión, tener un encabezado de extensión o varios encabezados de extensión. Existe un numero limitado de EHs en IPv6, cualquiera de las cuales puede aparecer solo una vez en el paquete. Los nodos que originan paquetes deben tener los EHs en un orden especifico, no así los que los reciben.
Cuando el campo Next Header contiene un valor que no se corresponde con un EH significa el fin de las cabeceras IPv6 y el comienzo de los datos.
Una implementación completa de IPv6 debe tener soporte para las siguientes cabeceras:

- Opciones Hop-by-Hop.
- Routing (tipo 0).
- Fragment.
- Destination options.
- Authentication
- Encapsulation Security Payload

Orden de los encabezados de extensión.
Los encabezados de extensión deben ser procesados la mayoría solamente por el destino y en el orden en que aparecen en el paquete, por lo que no afectan el desempeño de los routers.
El único encabezado que será procesado a lo largo de toda la ruta es el encabezado Hop-by-Hop options que debe seguir inmediatamente al encabezado IPv6 y ser identificado por un valor cero.
Cuando existen mas de un encabezado de extensión en un paquete, estos deben aparecer en el siguiente orden:

1. Cabecera básica IPv6 (IPv6 Header). Cabecera obligatoria.
2. Cabecera nodo por nodo (Hop-by-Hop Header options): Define opciones especiales que requieren procesamiento por los routers en cada salto. Definen rutas virtuales estáticas.
3. Cabecera opciones destino (Destination Options Header) si el encabezado de ruteo aparece. Opciones a ser procesadas por todos los nodos cuya dirección aparece en el campo dirección destino IPv6 y en el encabezado de ruteo.
4. Cabecera de ruteo extendido (Routing Header type 0): Ruta a seguir total o parcial. Proporciona un ruteo ampliado, similar al encaminamiento por la fuente de IPv4. Acarrea la información de ruteo para que no se detenga el trafico.
5. Cabecera de fragmentación y ensamblaje (Fragment Header): Contiene información de fragmentación y reensamblado. Optimiza los MTU en la capa de red, este MTU es de tamaño variable para permitir que la información importante llegue primero.
6. Cabecera de autenticación (Authentication Header): Verificación de la autenticidad del emisor. Proporciona la integridad del paquete y la autenticación. Comprueba

por efecto "Challenge" el perfil de usuario, se puede combinar con otros tipos de autentificación como el de PPP, de esta forma se realiza una autenticación mediante PPP e IP.

7. Cabecera de confidencialidad de datos (Privacy Header o Encapsulation Security Payload header): Cabecera de encapsulado de la carga de seguridad. Proporciona información sobre los tipos de mecanismos de seguridad usados para garantizar la confidencialidad e integridad del contenido cifrado en campo datos del datagrama. Encapsulamiento de puertos para negar acceso con puertos conocidos.
8. Cabecera de extremo a extremo (End to end Header): Control de flujo en la capa de red. Hace más eficiente la comunicación.
9. Cabecera de las opciones para el destino (Destination Options Header): Contiene información opcional a ser examinada solo por el nodo destino final.
10. Encabezado de capas superiores (Upper layer header) como TCP, UDP, ICMPv6, etc.

Cada una de estas cabeceras solamente debe aparecer una sola vez en el paquete, con excepción del encabezado opciones destino que puede aparecer dos veces en diferente posición..

Cuando los paquetes que incluyen algunos encabezados de extensión llegan al nodo destino, los encabezados deben ser procesados estrictamente en el orden en que aparecen en el paquete IPv6, no se puede procesar un paquete antes de procesar los que le anteceden.

Los encabezados Hop-by-Hop y Destination Options transportan numeros variables de opciones codificados en un formato TLV (Type-Length-Value), Fig. 3.4.3.2.

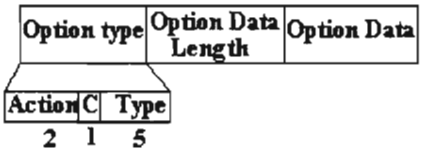


Fig. 3.4.3.2 Formato TLV.

Los campos del formato TLV son:

- Option Type: Entero de 8 bits sin signo que identifica el tipo de opción. Los dos primeros bits de mayor orden (Action) indican la acción a tomar si el nodo IPv6 no reconoce la opción, los valores de los bits Action, se muestran en la siguiente tabla:

Opción	Acción
00	Saltar esta opción y procesar las opciones subsecuentes.
01	Descartar el paquete y no enviar un mensaje ICMP
10	Descartar el paquete, indiferentemente si la dirección destino es multicast, se notifica al nodo fuente con un mensaje ICMP Unrecognized Type
11	Descartar el paquete, solamente si la dirección destino no es multicast, se notifica al nodo fuente con un mensaje ICMP Unrecognized Type

El tercer bit C (Change), solamente es usado por la cabecera Hop-by-Hop, especifica si el campo Option Data puede cambiar en la ruta al destino final del paquete, por esto solo las opciones hop-by-hop se pueden cambiar en la ruta, según los valores de la siguiente tabla:

0	Option data no puede cambiar en la ruta
1	Option data puede cambiar en la ruta y debe excluirse del checksum

Los 5 bits restantes definen la opción.

- Option Data Length: Entero sin signo de 8 bits que contiene la longitud del campo Option Data en octetos.
- Option Data: Campo de longitud variable que contiene el valor de la opción o los datos específicos del tipo de opción.

Cabecera de opciones Hop-by-Hop

La cabecera nodo por nodo contiene información opcional que es procesada por los distintos nodos y routers que se encuentran en el camino seguido por el paquete además del nodo destino, es usada por el Router Alert (RSVP y MLDv1) y el paquete jumbograma. Cada router debe procesar la opción así como también el encabezado IPv6 principal. Debe seguir a la cabecera principal y se identifica cuando el campo Next Header es igual a 0, este valor no es un numero de protocolo sino un caso especial para distinguir este tipo único de EH. Así por ejemplo la primera de sus opciones es definida para manejar paquetes IP extra grandes (jumbo payloads).

IPv6 puede mandar paquetes más grandes de 65,535 octetos sobre una red con valor de MTU muy grande. IPv4 no puede por que el campo Longitud Total es de 16 bits, IPv6 también tiene un campo de Payload de 16 bits, sin embargo usando un campo de 32 bits dentro del encabezado opciones salto por salto un paquete jumbograma puede tener una longitud máxima de 4,294,967,295 octetos.

Los encabezados de extensión en un paquete IPv6 no deben ser procesados por los routers intermedios, sin embargo la característica Router Alert puede ser usada cuando un paquete requiere procesamiento especial por los routers intermedios.

Los paquetes con jumbo payloads (con mas de 65535 bytes) requieren un tratamiento especial por que no todos los enlaces serán capaces de manejar unidades de transmisión de tamaño tan grandes y los routers evitan mandarlos a las redes que no los pueden manejar, el formato de esta cabecera es el siguiente:

Next Header	Header Ext Len	Options

Los campos de esta cabecera son:

- Next Header. Campo de 8 bits que identifica a la cabecera que le sigue.
- Header Ext Len. Indica la longitud de esta cabecera en múltiplos de 8 octetos, no incluye los primeros 8 octetos.
- Options. Campo de longitud variable y múltiplo de 8 octetos. Contiene una o varias opciones codificadas en TLV (Type Length Value). Inicialmente no estaban definidas opciones aparte de las de relleno.

Las opciones individuales en IPv6 se optimizan, para ello se alinean mediante dos opciones de relleno (padding):

- Pad1: Un solo byte se rellena mediante el byte X'00'. Las secuencias de relleno mayores se deberían efectuar con la opción PadN.
- PadN: Una opción en el formato TLV de valor X'01'. El correspondiente campo de longitud indica el numero de bytes de relleno después de los dos requeridos como mínimo.

Opción Jumbo Payload

Debido a que el campo Payload Length de 16 bits en el encabezado IPv6 limita la longitud de la carga útil a 65,535 bytes, la opción Jumbo Payload puede ayudar a exceder este limite, el formato de esta opción se muestra en la Fig. 3.4.3.3.

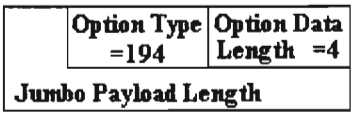


Fig. 3.4.3.3 Formato de la opción Jumbo Payload

Los campos de la opción Jumbo payload son:

- Option type: Campo de 8 bits de valor 194 que identifica la opción 194.
- Option data length: Campo de valor 4 que indica que 4 octetos de datos seguirán (campo Jumbo Payload).
- Jumbo Payload Length: Indica la longitud del paquete en octetos, excluyendo el encabezado IPv6 pero incluyendo el encabezado Hop-by-Hop. Esta longitud debe ser de mas de 65535 bytes.
  El campo Payload Length en el encabezado IPv6 debe ser puesto a cero en cada paquete que transporte la opción Jumbo Payload.

Cabecera opciones destino

Este encabezado de valor 60 sigue al encabezado salto por salto, este encabezado es procesado solamente por el nodo o nodos destino, no por cada nodo en la trayectoria de ruteo del paquete. Transporta información opcional que esta específicamente dirigida a una dirección destino. El formato de este encabezado se muestra en la Fig. 3.4.3.4

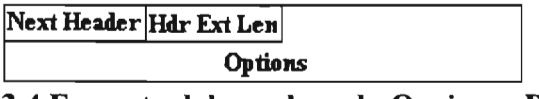


Fig. 3.4.3.4 Formato del encabezado Opciones Destino.

Sus campos son:

- Next Header: Campo de 8 bits que identifica el encabezado que le sigue.
- Hdr Ext Len: Campo de 8 bits que contiene la longitud del encabezado de ruteo en unidades de 8 octetos (64 bits), no incluyendo el primer campo.
- Options: Campo de longitud variable que contiene una o más opciones TLV codificadas.

IP móvil usa este encabezado. La especificación del protocolo IPv6 móvil propone el uso del encabezado opciones destino para intercambiar mensaje de registro entre nodos móviles y el agente local.

Cabecera de Ruteo.

Este encabezado es usado para forzar a un paquete a que pase a través de routers específicos en el camino a su destino. Esta cabecera es similar a la opción Loose Source Routing de IPv4.

En la cabecera de ruteo el emisor IP establece una lista de nodos intermedios que deberá seguir el paquete para llegar a su destino con el campo Routing Type puesto a cero. La especificación puede ser para cada uno de los nodos en la ruta obligatoria (Strict) o no (Loose). Esta cabecera soporta el protocolo de ruteo a petición del emisor (Source Demand

Routing Protocol, SDRP), esta cabecera se identifica con el valor 43 en el campo Next Header precedente, el formato de esta cabecera se muestra en la Fig. 3.4.3.5

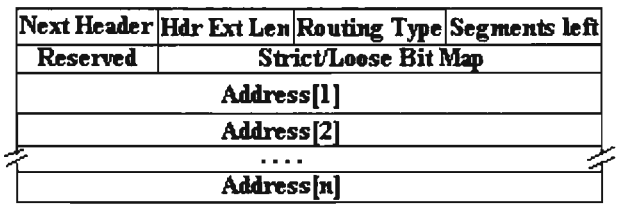


Fig. 3.4.3.5 Campos de la cabecera de ruteo (encaminamiento)

Los campos de esta cabecera son:

- Next Header: Campo de 8 bits que indica el tipo de cabecera que le sigue.
- Hdr Ext Len: Campo de 8 bits que contiene la longitud del encabezado de ruteo en unidades de 8 octetos (64 bits), no incluyendo el primer campo, en el caso del ruteo tipo 0 este campo debe ser menor o igual a 46, igual a dos veces el numero de direcciones en el encabezado. Los primeros 64 bits contienen la parte fija del encabezado de ruteo tipo 0 (Next Header, Hdr Ext Len, Routing type, Segments left, reserved, Strict/Loose Bit Map) y cada una de las direcciones tiene 128 bits, esto es, dos veces 64 bits.
- Routing type: Este campo de 8 bits siempre vale 0. Diferentes valores pueden ser usados en el futuro para soportar diferentes encabezados de ruteo. El tipo de ruteo 0 forza el ruteo a través de una lista de routers intermedios.
- Segments Left: Este campo de 8 bits identifica el numero de routers intermedios que están en la porción datos del encabezado de ruteo, que son el numero de nodos intermedios explícitamente listados para ser visitados en la ruta al destino, esto es, el numero de direcciones todavía sin usar. El valor máximo para este campo es 23.
- Reserved: Campo reservado para uso futuro. Tiene un valor de 0 para la transmisión, es ignorado por el receptor.
- Strict/Loose Bit Mask: Con este campo de 24 bits un nodo opta por un camino. Este campo es una mascara que contiene un bit Strict/Loose por cada dirección. Si el bit Strict/Loose asociado con una dirección es 0, la dirección debe ser tratada como loose si es igual a 1 la dirección debe ser tratada como Strict.

Cada campo de dirección es de 128 bits de largo y hasta 23 campos de dirección pueden ser usados. Estos campos contienen las direcciones IPv6 de los nodos a ser atravesados a lo largo de la ruta al destino. Los nodos son visitados en el orden numérico listado.

Cuando el encabezado de ruteo es procesado por un nodo, el nodo checa si el campo segments left es diferente de 0, si es así extrae la siguiente dirección y el bit asociado Strict/Loose, si el bits indica que la dirección de debe ser tratada en con la opción Strict, se checa que la dirección pertenezca a un nodo adyacente (un vecino en uno de los enlaces) y se entrega el paquete a la interfaz asociada a ese nodo, si el nodo no es adyacente se desecha el paquete. Si se indica que la dirección debe ser tratada en la forma Loose, el nodo examina su tabla de ruteo y rutea el paquete a la dirección.

Cuando la lista de routers IPv6 intermedios es creada el nodo fuente ejecuta las siguientes operaciones:

1. Pone al primer router de la lista de routers intermedios la dirección destino en el encabezado IPv6 básico en lugar del destino IPv6 original.
2. Pone al destino IPv6 original como el destino final de la lista de routers intermedios.

3. Decrementa por 1 el campo Segments Left del encabezado de ruteo conforme el paquete pase a través de cada router. Dicho campo es un apuntador que contiene el numero restante de segmentos de router al destino original.

Por su parte en cada router intermedio de la lista se ejecutan los siguientes pasos:

a) El router intermedio cambia la dirección destino del encabezado IPv6 básico para apuntar al siguiente router en la lista de routers intermedios.
b) El router decrementa por 1 el campo Segments Left de encabezado de ruteo.
c) El router pone su propia dirección en la lista de routers en el encabezado de ruteo antes del siguiente router (para registrar la ruta).
d) Si el router es el ultimo en la lista de routers intermedios cambia la dirección IPv6 destino del encabezado IPv6 básico a la del nodo destino final, el cual es el destino original del paquete.

Cuando el nodo destino recibe el paquete con el encabezado de ruteo puede ver la lista de routers intermedios registrada en el encabezado de ruteo, Fig. 3.4.3.6 y de esta forma puede responder los paquetes al nodo fuente usando el encabezado de ruteo para especificar la misma lista en orden inverso

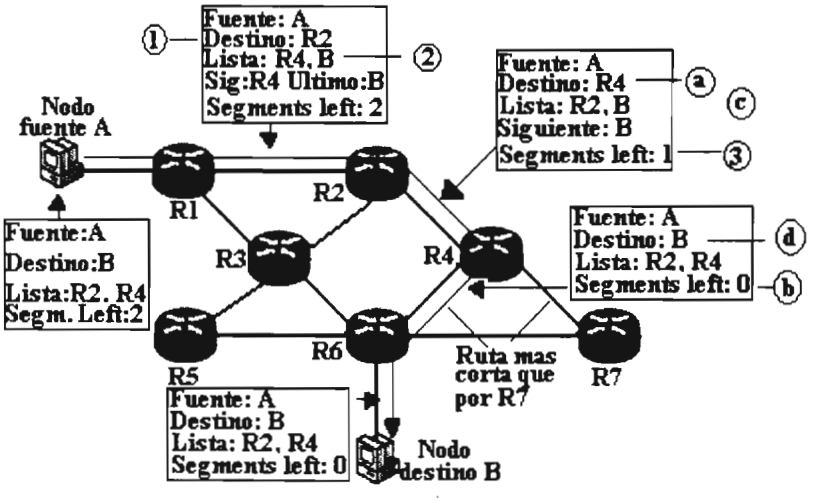


Fig. 3.4.3.6 Uso de la cabecera de ruteo.

Esta cabecera es usada para ruteo fuente e IPv6 móvil. La movilidad IPv6 usa el encabezado de ruteo cuando un nodo esta lejos de su red, ya que este le proporciona eficiencia.

Cabecera de Fragmentación

En IPv6 la fragmentación es indeseable, por lo que lo ideal seria que los nodos fuente no realizaran fragmentaciones de los paquetes, y definitivamente no se permite la fragmentación en los routers (a diferencia de IPv4 que sí lo permite). Por ello se usa el mecanismo de descubrimiento de unidad máxima de transmisión de la ruta PMTUD, mecanismo con el cual, el nodo descubre desde antes de mandar el paquete cual es el MTU más pequeño de toda la trayectoria, para que en base a ese valor, se manden los paquetes desde la fuente y no se tenga necesidad de fragmentar los paquetes. Para esto el nodo debe soportar el mecanismo PMTUD, cuando un nodo no soporta PMTUD y debe mandar un paquete más grande que el MTU de la trayectoria de entrega, la fragmentación tiene que ser usada por medio del encabezado de fragmentación.

El nodo fuente debe fragmentar un paquete que es más grande que la unidad de transmisión máxima (MTU) de la trayectoria entre dicha fuente y el dispositivo destino, este encabezado (fragmentación) será incluido en cada paquete fragmentado. El nodo fuente divide el paquete en fragmentos, transmite cada fragmento en un paquete separado e identifica los fragmentos agregando el encabezado de fragmentación a los encabezados IPv6. Los paquetes fragmentados tienen una extensión en vez de información en la cabecera IPv6. Esto reduce el tamaño de la cabecera IPv6. Debido a que los protocolos de alto nivel como TCP tienden a evitar la fragmentación de datagramas se reduce el overhead para la cabecera IPv6 en casos normales.
El emisor IP usa esta cabecera para mandar paquetes de tamaño superior al que se pueden enviar a un destinatario. Esta cabecera se distingue por un valor del campo Next Header igual a 44, el cual se encuentra después de la cabecera anterior.
La fragmentación solo es ejecutada por los nodos origen y no por los ruteadores que intervengan en la trayectoria, en IPv6 los ruteadores funcionan como si el bit de fragmentación de IPv4 indicara que no se debe realizar fragmentación, por lo que al recibir un paquete mayor al MTU del enlace por el que lo deben retransmitir, desechan el paquete y mandan un mensaje ICMP a la fuente indicándole la longitud máxima que puede tener el paquete, entonces la fuente procederá a reenviar el paquete fragmentándolo primero. Así los únicos nodos que necesitan estar preocupados de las cabeceras de extensión de fragmentación son el nodo fuente y el nodo destino. El nodo fuente hace la fragmentación y crea los encabezados, los cuales son puestos después del encabezados IPv6 principal y antes del siguiente encabezado del protocolo de capa superior. El nodo destino acepta el paquete y usa el encabezado extensión de fragmentación para reensamblar el paquete. Todos los nodos intermedios pueden ignorar los encabezados extensión de fragmentación, así mejora la eficiencia conforme los paquetes son ruteados.
Los campos de esta cabecera se muestran en la Fig. 3.4.3.7:

Next Header	Reserved	Fragment offset	Reserved	M
Identification				

Fig. 3.4.3.7 Formato del encabezado-extensión para la fragmentación.

Sus campos son:

- Next Header: Campo de 8 bits que indica el tipo de cabecera que le sigue.
- Reserved: Campo de 8 bits para uso futuro, inicializado a cero para la retransmisión, es ignorado por la recepción.
- Fragmentation offset: Es un entero sin signo de 13 bits que indica la posición del fragmento especifico en el paquete IP original completo. El primer fragmento esta en el lugar numero 0. Este campo tiene un valor múltiplo de 8 octetos.
- Reserved: Campo de 2 bits con valor 00 puesto a cero por la transmisión e ignorado por el receptor.
- M: Este campo de 1 bit indica si quedan mas fragmentos cuando esta a 1. Cuando esta a cero indica que no queda ningún fragmento.
- Identification: Campo de 32 bits que contiene un identificador único del paquete generado por el nodo que realiza la fragmentación. Identifica fragmentos pertenecientes al mismo al mismo paquete original. Permite identificar el datagrama para asegurar el reensamblaje de los paquetes. Este numero esta contenido en la cabecera de todos los fragmentos del mismo datagrama. Es similar al de IPv4 pero dos veces mas largo.

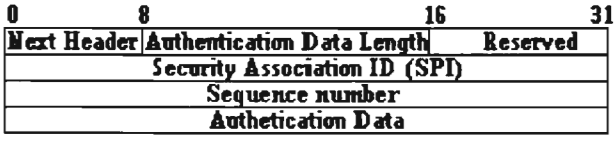
El paquete IPv6 consiste de dos partes:

- Parte no fragmentable: Consiste de encabezado IPv6 más otros encabezados que deben ser procesados por todos los nodos a lo largo de la ruta (encabezados de extensión hasta e incluyendo el encabezado de ruteo).
- Parte fragmentable: Es el resto del paquete como los encabezados de extensión a ser procesados solamente por el destino y la carga útil IPv6.

La parte fragmentable se divide en fragmentos múltiplos de 8 octetos a excepción del ultimo. Un encabezado de fragmentación es puesto antes de cada fragmento y cada fragmento se transmite como un paquete IPv6 separado.
El nodo destino debe reensamblar los fragmentos en el orden indicado por el campo fragment offset.

Cabecera de autenticación

Este encabezado se usa en IPSec para proporcionar autenticación, integridad de los campos IP que no cambian en la ruta y protección contra repeticiones. La autenticación tiene como algoritmos básicos para su funcionamiento el MD-5 codificado y el SHA-1. En el campo Next Header del encabezado principal su valor es de 51, sus campos se observan en la siguiente figura:



Los campos de la cabecera de autenticación son:

- Next Header: Identifica el tipo de cabecera que le sigue. Los valores son iguales a los del campo Protocol de IPv4.
- Authentication Data Length: Longitud del campo Authentication data en múltiplos de 8 octetos.
- Reserved: Tiene un valor 0, es ignorado por el receptor.
- Security Association ID: Es un valor arbitrario de 32 bits que junto con la dirección IP destino y el protocolo de seguridad AH identifica la asociación de seguridad SA para el datagrama.
- Sequence number: El numero de secuencia es un campo de 32 bits sin firmar que contiene el valor de un contador que se incrementa.
- Authentication Data: Indica el algoritmo que se usa para autentificar el origen del paquete y para asegurar su integridad respecto al tipo de seguridad asociado. Todos los nodos IPv6 han de soportar un algoritmo mínimo. Este campo tiene una longitud variable múltiplo de 8 octetos que contiene el valor de comprobación de integridad ICV (Integrity Check Value).

La autenticación permite proteger contra las siguientes amenazas:

- Detectar cambios en el contenido de la información (modificación de los campos fijos).
- El receptor puede verificar la identidad del transmisor.
- Se pueden evitar los ataques por engaño de IP (packet spoofing).
- Se puede proporcionar protección contra ataques de repetición (flooding o replay).

Este encabezado es también conocido como el encabezado AH de autenticación IPSec.

Cabecera de autenticación IPv6 (Cabecera encapsulada de seguridad IPv6)

IPv6 ofrece la posibilidad de solucionar los problemas de seguridad (confidencialidad y autentificación por debajo del nivel de aplicación) proporcionando dos opciones integradas que conllevan seguridad. Las dos opciones pueden ser usadas independientemente o al mismo tiempo según las necesidades que se tengan.

Esta opción proporcionara autenticación e integridad pero no confidencialidad. La opción será independiente de algoritmos y soportara varias técnicas de autenticación.

El uso de keyed MD se ha propuesto para asegurar interoperabilidad dentro de Internet

Esta opción dará integridad y confidencialidad ausentes en la opción de cabecera de autenticación de IPv6.

El algoritmo DES ha sido propuesto como el estándar con el fin de conseguir interoperabilidad en Internet.

Cabecera de confidencialidad

El encabezado ESP de valor 50 es usado en IPSec para proporcionar integridad, confidencialidad, autenticación y protección contra repeticiones del origen de un paquete. Evita el acceso no autorizado al paquete, encriptando los datos y colocándolos en la parte correspondiente de la cabecera de confidencialidad. Se puede solamente encriptar la trama del nivel de transporte o el datagrama entero. Esta cabecera es siempre el ultimo campo no encriptado de un paquete. Funciona entre estaciones, entre una estación y un firewall o entre firewalls. Los campos de esta cabecera son:

<table>
<tr><td colspan="3">Security Association Identifier</td></tr>
<tr><td colspan="3">Initialization Vector</td></tr>
<tr><td>Next Header</td><td>Length</td><td>Reserved</td></tr>
<tr><td colspan="3">Protected Data</td></tr>
<tr><td colspan="3">Trailer</td></tr>
</table>

Campos de la cabecera de confidencialidad:

- Security Association Identifier (SAID): Identifica el tipo de seguridad del datagrama. Si no hay ninguna asociación de seguridad el valor de este campo es 0x0000. Las asociaciones son en un solo sentido, por lo que en una comunicación confidencial entre dos nodos debe haber dos SAID, uno para cada sentido. La estación destino distingue la asociación correcta mediante la combinación del valor del SAID y la dirección fuente.
- Initialization Vector: Campo opcional, cuyo valor depende del SAID usado.
- Next Header: Campo encriptado que identifica el tipo de cabecera que le sigue. Los valores son idénticos a los del campo Protocol de IPv4.
- Reserved: Valor encriptado que es ignorado por el receptor.
- Length: Campo encriptado que indica la longitud de la cabecera codificada, no incluye los 8 primeros octetos, es un múltiplo de 8 octetos.
- Protected Data: Campo encriptado que puede contener encapsulado un datagrama IPv6 completo, una secuencia de opciones IPv6 y el paquete del nivel de transporte.
- Trailer: Campo encriptado usado de relleno o para registrar datos de autentificación usados en un algoritmo de criptografía que proporcione confidencialidad sin autentificación.

Este encabezado proporciona encapsulación de los datos con encripción para asegurar que solo el nodo destino puede leer la carga útil transportada por el paquete IP. Este encabezado debe ser siempre el ultimo ya que oculta tanto la carga útil del nivel superior como los siguientes encabezados. Este encabezado también es conocido como encabezado ESP de encapsulamiento IPSec.

Cabecera de extremo a extremo (Header End-to-End)
Esta cabecera tiene el mismo formato que la cabecera Hop-by-Hop. Proporciona información que debe ser controlada o examinada solo por el o los nodos destinatarios del paquete. Es identificada por un valor del campo Next Header TBD que sigue a la cabecera previa, su formato es igual al de la cabecera de opciones nodo por nodo, con la excepción de excluir una opción de calculo de la integridad de autentificación.
Capacidad de etiquetamiento de flujo: Una nueva capacidad ha sido agregada para habilitar el etiquetamiento de paquees pertenecientes a un flujo de trafico particular para el cual el transmisor solicita un manejo especial tal como calidad de servicio no por default o servicio en tiempo real.
Inexistencia de siguiente encabezado.
Cuando en el campo Next Header del encabezado IPv6 se tiene un valor 59, indica que no sigue ningún encabezado. Si el campo Payload Length indica otros octetos después del encabezado, estos se deben ignorar y retransmitir sin cambio.

Encabezado de capas superiores
Los encabezados de capas superiores o de transporte son los que se encapsulan dentro de un paquete para transportar los datos. Los dos protocolos de transporte principales son TCP con valor 6 y UDP con valor 17.
Encabezado TCP en IPv6
El protocolo de control de transmisión TCP con valor 6 es considerado un protocolo de capa superior tanto en IPv4 como en IPv6 y debido a que es un protocolo muy complejo no sufrió ninguna modificación para IPv6.
Encabezado UDP en IPv6
El protocolo de datagramas de usuario UDP que tiene un valor de 17 es también considerado un protocolo de capa superior tanto en IPv4 como en IPv6, este protocolo no ha cambiado para IPv6, sin embargo el campo checksum que en IPv4 era opcional, es obligatorio en IPv6, como muestra la Fig. 3.4.3.8.

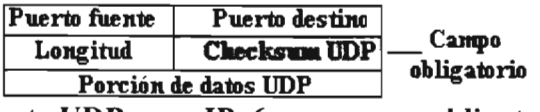


Fig.3.4.3.8 Paquete UDP para IPv6 con campo obligatorio Checksum.

Por lo que el campo checksum debe ser calculado por los nodos fuente IPv6 antes de ser transmitido.

IPv6 permite la encapsulación de IPv6 en IPv6 (tunneling). Esto se hace con un valor 41 para el campo Next Header. El paquete IPv6 encapsulado puede tener sus propias EHs. Los routers no deberían agregar EHs a los paquetes, sino encapsularlos en paquetes propios

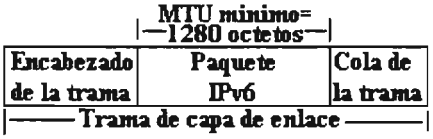
(fragmentados, si hace falta) ya que el tamaño de cada paquete se ha calculado en el nodo originador para que se ajuste al PMTU.

Tamaño de los paquetes MTU

El MTU es el tamaño de paquete máximo en bytes que una interfaz particular puede manejar.

En IPv4 la longitud del MTU mínimo de un enlace es de 68 octetos, por lo que cada equipo debe ser capaz de enviar paquetes IPv4 de 68 bytes sin fragmentación. Como la longitud máxima de un encabezado IPv4 es de 60 octetos, el tamaño de fragmento mínimo es de 8 octetos.

La longitud del MTU mínimo en un enlace IPv6 es de 1280 octetos.



El mínimo datagrama soportado es el tamaño de datagrama después del ensamblaje de la capa IP por parte de la implementación IP.

En IPv4 la longitud mínima del datagrama soportado es de 576 octetos.

En IPv6 la longitud mínima del datagrama soportado es de 1280 octetos.

En las primeras especificaciones de IPv6 se planteaba que los nodos IPv6 determinaran dinámicamente la PMTUD (Path Maximum Transfer Unit Discovery) de cada enlace y así los nodos fuente solo enviarían paquetes que no excedieran el tamaño del PMTU más pequeño. Por esto los routers IPv6 no tendrán que fragmentar paquetes a la mitad de rutas con mas de un salto y permitirán hacer un uso mucho más eficiente de las rutas. Inicialmente se había propuesto que cada enlace soportara una MTU mayor o igual a 576 bytes para permitir a IPv6 operar correctamente. Si algún enlace no puede cumplir con esto debe poder realizar la fragmentación en la capa de enlace o capa 2 del modelo OSI.

Los enlaces que tengan un MTU configurable deben ser configurados para tener un MTU mayor que o igual a 576 bytes.

Por lo anterior lo recomendable es que los nodos IPv6 implementen el descubrimiento de PMTU para poder usar MTU´s mayores a 576 bytes, para nodos simples que no pueden realizar esto, con mandar paquetes no mayores a 576 bytes aseguraran que dichos paquetes se adecuen al MTU de la ruta y puedan ser entregados.

Los paquetes IPv6 son transportados sobre Ethernet con el contenido tipo (content type) 86DD en hexadecimal, en lugar del 0800 de IPv4. El tamaño máximo del paquete soportado por el encabezado IPv6 es de 65,536 octetos, el cual esta limitado por la longitud de 16 bits del campo Payload. Sin embargo con el uso del encabezado de extensión los paquetes más grandes o jumbograms son posibles en IPv6. De esta forma se podría manejar un paquete jumbogram de hasta 4,294,967,295 octetos en comparación con el MTU de la tecnología 10 GB Ethernet, el cual es de 9216 octetos.

3.4.4 Direcciones IPv6

El esquema de direccionamiento en IPv6 sigue las siguientes directrices:

- Un numero mayor de bits para que el espacio de direccionamiento no este sujeto a un nuevo agotamiento.
- Una organización jerárquica más flexible de direcciones que no usen el concepto de clases, sino el mecanismo CIDR.
- Un esquema para la asignación de dirección que apunte a minimizar el tamaño de las tablas de ruteo en los routers e incremente el desempeño CIDR.
- Direcciones globales para el Internet y direcciones locales para las Intranets.

El sistema de direcciones de la versión 6 tiene una longitud 128 bits (16 octetos), por lo que son cuatro veces mayor que las de 32 bits de IPv4.

El por que de usar 128 bits se debe a la medida para medir la eficiencia de la asignación de dirección H, esta medida se define la razón entre el logaritmo en base 10 de numero de direcciones usadas y el numero de bits de la dirección:

$$H=\frac{\log_{10}(\text{numero direcciones})}{\text{Bits numero}}$$

Para un esquema de máxima eficiencia donde todas las direcciones son usadas $H = \log_{10} 2 = 0.301$.

En esquemas de direccionamiento real H varia entre 0.22 y 0.26.

Para un millón de billón (10^{15}) de computadoras en red, el peor caso de H=0.22 requiere direcciones de 68 bits, como las direcciones deben ser múltiplos de 32 bits se opto por los 128 bits.

A diferencia de IPv4 cuyas direcciones se encuentran organizadas estrictamente en clases de direcciones, Las direcciones IPv6 están diseñadas para ser usadas con CIDR (Classless Interdomain Routing). El enorme espacio de direcciones IPv6 puede cubrir un amplio rango de espacios de direcciones existentes y propuestos. La estrategia de IPv6 análoga a CIDR, consiste en utilizar parte de la dirección, por ejemplo el primer byte, para indicar el tipo de dirección. Estos tipos incluirán un mapeado del espacio IPv4 a IPv6, OSI NSAPs, Novell IPX, etc.

El aumento en el espacio de direcciones no solo proporciona mayor numero de hosts, sino una jerarquía de direcciones mayor.

Las nuevas direcciones identifican a un interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, se puede referir a estos a través de su interfaz. Una única interfaz puede tener múltiples direcciones monodestino. Cualquiera de las direcciones monodestino asociadas a las interfaces de los nodos se puede utilizar para identificar de forma univoca al nodo.

El número de direcciones diferentes que se pueden obtener y utilizar con 128 bits es muy grande ya que se tendrían 2^{128} direcciones posibles sin aplicar algún formato u organización a estas.

Se pueden llegar a soportar mas de 665,000 trillones de direcciones distintas por cada metro cuadrado de la superficie de la Tierra.

Una vez organizadas estas direcciones de forma practica y jerárquica quedarían reducidas en el peor de los casos a 1,564 direcciones por cada metro cuadrado y siendo optimistas se pueden alcanzar entre tres y cuatro trillones.

IPv6 soporta mas niveles de direccionamiento jerárquico, un numero mucho más grande de nodos direccionables y una autoconfiguración de direcciones más simple.
Además de acrecentar el espacio de direcciones de 32 bits a128 bits, la arquitectura de direccionamiento IPv6 hace algunos ajustes a los diferentes tipos de direcciones disponibles para un host IP. Se especifican direcciones unicast para una sola interfaz de red y las direcciones multicast especifican una dirección a la cual uno o más hosts pueden estar escuchando, este tipo de direcciones continua básicamente sin cambio desde IPv4. IPv6 elimina las direcciones de broadcast.
Escalabilidad de direcciones multicast. Un nuevo tipo de dirección llamada dirección anycast es también definida para mandar un paquete a alguno de un grupo de nodos. Por lo tanto las características de las direcciones IPv6 son:

- Las direcciones IPv6 especifican la parte que representa a la dirección de red con el concepto CIDR, es decir se usa un prefijo y la longitud del prefijo.
- La estructura de campos de la dirección IPv6 permite la asignación jerárquica. De este modo con la representación CIDR y la estructura en campos las direcciones pueden ser agregadas fácilmente lo que disminuye el tamaño de las tablas de ruteo.
- Las direcciones son asignadas a interfaces (y varias) no a un nodo.
- Las direcciones IPv6 no pueden hacer broadcast.

3.4.4.1 Representación de direcciones IPv6

En las direcciones IPv6 la notación decimal con puntos que separan campos de 8 bits seria impractica, como por ejemplo con la siguiente dirección:
104.230.140.100.255.255.255.255.100.17.100.128.150.10.255.255
Esta forma de representar una dirección de 128 bits además de ser impractica es engorrosa, difícil de manejar y recordar.
IPv6 usa direccionamiento de 128 bits expresados en formato hexadecimal, para las direcciones IPv6 se decidió representarlas con 8 grupos de dígitos hexadecimales agrupados de cuatro en cuatro (cada agrupación contiene 16 bits) y separados cada grupo de 4 dígitos hexadecimales mediante el símbolo dos puntos (:).
Este formato general de las direcciones IPv6 se muestra en la Fig. 3.4.4.1.1

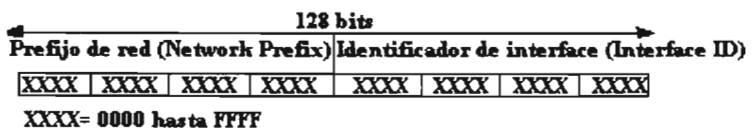
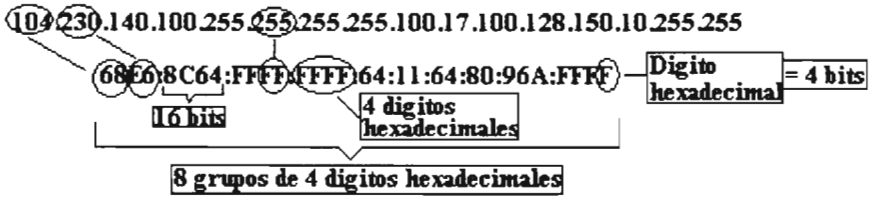


Fig.3.4.4.1.1 Formato de la dirección IPv6

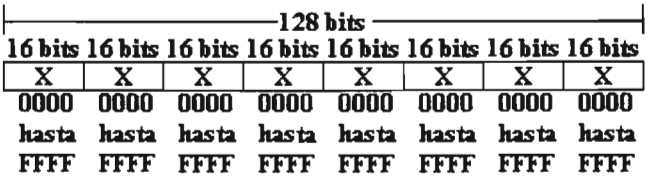
Donde X= digito hexadecimal con valor desde 0 a F
De esta manera la dirección anteriormente mencionada en formato decimal queda representada de la siguiente forma:



Existen tres formas convencionales de representar las direcciones IPv6:

1. **Forma normalizada.**

La forma normalizada o preferida es la forma mas aceptada de representar las direcciones IPv6 y es también el formato mas largo, ya que representa todos los 32 caracteres hexadecimales que forman una dirección IPv6. Este es un formato hexadecimal de ocho campos de números en forma hexadecimal cada uno representando a un conjunto de 16 bits (2 octetos) y separado cada campo con el signo dos puntos (:), es decir, se forman 8 grupos de dos octetos cada uno, como se muestra a continuación:



Donde:

Cada campo de 16 bits es representado por 4 caracteres hexadecimales. Las X representan los valores hexadecimales de los ocho bloques de dos octetos (16 bits) cada uno.

El valor de cada campo de 16 bits puede tener valores hexadecimales desde 0x0000 hasta 0xFFFF.

Por ejemplo tenemos las siguientes direcciones:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417C

En este caso los primeros 4 octetos son el prefijo y los 4 restantes son el Interface ID.

Hay que destacar de estos ejemplos que no es necesario escribir todos los ceros en un campo individual pero por lo menos ha de haber una cifra en cada campo. Es decir se pueden omitir los ceros a la izquierda en un campo dado.

2. **Forma de representación de ceros consecutivos.**

Esta es la forma comprimida de una dirección. El método de asignación de direcciones por comodidad coloca bits a 0, por lo que es común tener largas cadenas de ceros en medio de las direcciones y para facilitar la escritura de direcciones IPv6 a las personas una sintaxis adecuada seria suprimir esos ceros. De esta forma se tienen dos sintaxis especiales cuando se tienen valores 0´s:

- Los primeros bits de un campo de 16 bits son ceros.
- Campos de 16 bits sucesivos compuestos de 0´s.

- **Los primeros bits de un campo son cero.**

Este método de representación se aplica a cada campo hexadecimal de 16 bits en el cual uno o más de los primeros bits es cero. Los primeros bits de cada campo con valor cero pueden ser removidos. Si el campo entero esta compuesto de puros 0´s al menos un valor cero debe ser puesto.

Como ejemplos de esta representación simplificada tenemos:

- FFC1:0000:0000:0000:0000:0000:0000:0101=FF01: 0:0:0:0:0:0:101
- 0000:0000:0000:0000:0000:0000:0000:0001=0:0:0:0:0:0:0:001
- 0000:00000:0000:0000:0000:0000:0000:0000=0:0:0:0:0:0:0:0

- **Campos de 16 bits sucesivos compuestos de 0´s.**

Cuando se tiene uno o varios campos con valor cero en una dirección estos pueden ser reemplazados por una pareja de dos puntos (: :), esta sustitución podrá ser realizada una sola vez en una misma dirección.
Como ejemplos de esta representación simplificada tenemos:

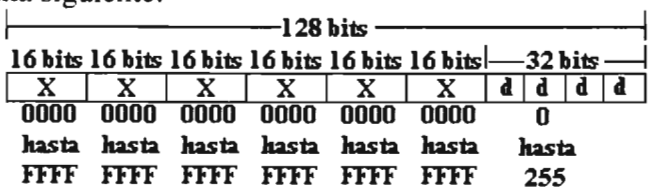
- FF01:0000:0000:0000:0000:0000:0000:0101=FF01: :0101
- 0000:0000:0000:0000:0000:0000:0000:0001=: :0001
- 0000:00000:0000:0000:0000:0000:0000:0000=: :

Estas dos ultimas formas de representar una dirección se pueden mezclar para hacer la representación de una dirección IPv6 más corta. Así tenemos en los anteriores ejemplos:

- FF01:0000:0000:0000:0000:0000:0000:0101=FF01: :101
- 0000:0000:0000:0000:0000:0000:0000:0001=: :1
- 0000:00000:0000:0000:0000:0000:0000:0000=: :

3. Forma de representación de direcciones mixtas.

Este método esta relacionado a los mecanismos de transición donde una dirección IPv4 es insertada en una dirección IPv6. En esta forma de representación la primera parte de la dirección IPv6 usa la representación hexadecimal y la parte de la dirección IPv4 esta en formato decimal.
Cuando estamos en un ambiente mixto de nodos IPv6 e IPv4 las direcciones se pueden representar en la forma siguiente:



Estas direcciones se componen de los seis campos de mayor orden, las X con valores hexadecimales (6 grupos de 16 bits), seguidos de los 4 campos de mas bajo orden, las d con valores decimales (4 grupos de 8 bits en la representación estándar de IPv4).
Estas a su vez se dividen en dos clases de direcciones IPv6 con direcciones IPv4 insertadas que se diferencian en el prefijo usado por cada dirección IPv4 insertada:

- Direcciones IPv6 compatibles-IPv4.
  Usadas básicamente por los mecanismos de transición para establecer túneles automáticos para transportar paquetes IPv6 sobre redes IPv4. En este tipo el prefijo compuesto de los 96 bits de mas alto orden es puesto a 0, seguidos de los 32 bits de la dirección IPv4. Así por ejemplo tenemos:

0:0:0:0:0:0:13.1.68.3= ::13.1.68.3
0:0:0:0:0:0:0D01:4403= ::D01:4403

- Direcciones IPv6 mapeadas-IPv4.
  Usadas solamente en el ámbito local de los nodos que manejan ambos protocolos IPv6/IPv4. Por lo que son de uso interno. En este tipo el prefijo de los 80 bits de mas alto orden es puesto a cero, los siguientes 16 bits son puestos a 1 seguidos de los 32 bits de la dirección IPv4.

Así por ejemplo tenemos:
0:0:0:0:0:FFFF:13.1.68.3= ::FFFF:13.1.68.3
0:0:0:0:0:FFFF:0D01:4403= ::FFFF:D01:4403

Esta representación es útil solamente si sé esta usando mecanismos de transición como los túneles automáticos compatibles con IPv4 y los mecanismos de traducción NAT-PT.

3.4.4.2 Prefijo del formato de dirección IPv6 y subnetting.

En IPv6 la estructura de las direcciones se compone de dos partes que son el prefijo y el identificador de interfase:

Dirección IPv6=Prefijo+Identificador_Interface

Donde:

- El prefijo (prefix) va a depender de la topología de ruteo, nos indica en donde estas conectado.
- El identificador de la interfase (interface ID) identifica un nodo, indica quien eres.

- **El prefijo**

En las direcciones IPv6 el primer campo de longitud variable de bits es denominado el prefijo del formato FP (Format Prefix) que permite identificar el tipo de dirección de IPv6.
El prefijo de las direcciones IPv6 es el equivalente de las mascaras de subred de IPv4. Indica cuantos bits son usados para identificar la subred. En IPv4 se tienen dos formas para representar un prefijo de red:

- Notación decimal.
  La mascara de red se representa en forma decimal punteada d.d.d.d. Este valor representa el numero de bits consecutivos que son puestos a 1. Por ejemplo para una dirección con prefijo 192.168.1.0 el valor de la mascara de red es 255.255.255.0
- Notación CIDR (Classless Interdomain Routing).
  La mascara de red puede ser representado con un numero decimal que indica el numero de bits consecutivos puestos a 1. El carácter diagonal es usado entre el prefijo y la mascara de red. Para el ejemplo anteriormente mencionado el prefijo se representa como 192.168.1.0/24.

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4. Aunque las direcciones IPv6 se representan en formato hexadecimal, el valor de la mascara de red se representa en forma decimal
Por lo tanto un prefijo de dirección IPv6 se representa con la siguiente notación:

Dirección IPv6/longitud del prefijo

- Dirección IPv6: Es una dirección IPv6 en cualquiera de sus formas de presentación (8 campos hexadecimales de 16 bits, representación simplificada de ceros. representación de direcciones mixtas).
- Longitud del prefijo: Es un valor decimal que especifica cuantos de los bits más significativos representan el prefijo de la dirección.

Con el uso del FP las líneas que identifican a una dirección y a su prefijo se pueden combinar en una sola línea indicando el mismo concepto, así las líneas:

- Dirección de nodo: FEC0:0:0:3:CDFF:FEA9:528B
- Prefijo: FEC0:0:0:3::/64

Se pueden combinar en una sola como:

- FEC0:0:0:3: CDFF:FEA9:528B::/64

Los prefijos de una dirección donde toda la parte de Interfase ID es cero se pueden representar también en forma más sencilla, de esta forma si el prefijo de una dirección tiene la forma:
3FFE:0000:0000:CD30:0000:0000:0000:0000/60
Este se puede representar de las dos siguientes formas:
3FFE::CD30:0:0:0:0/60
3FFE:0:0:CD30::/60
Con esta notación la representación de direcciones IPv6 y prefijos de red usando la notación CIDR son:

Prefijo IPv6	Descripción
FE80::20B:CDFF:FEA9:528B/128	Prefijo de una subred con una sola dirección IPv6
FEC0:0:0:3/64	Prefijo de red que puede manejar 2^{64} nodos. Esta es la longitud del prefijo por default de una subred.
2002:C000:51::/48	Prefijo de red que puede manejar 2^{16} prefijos de subred de 64 bits cada uno. Esta es la longitud del prefijo por default para un sitio.

Tanto en IPv4 como en IPv6 el numero de bits puestos a 1 en la mascara de red define la longitud del prefijo de red, la parte restante es para el direccionamiento de nodos.
El tipo de dirección es identificado por el prefijo del formato. Un valor de 11111111 (FF) para el FP identifica una dirección como dirección de multicast. Cualquier otro valor en los bits de mayor orden identifica la dirección como dirección unicast.
En IPv6 no existen direcciones reservadas dentro de los rangos de subred como en IPv4 (dirección de red y dirección de broadcast). En IPv6 el numero de bits para el direccionamiento de nodos es tan grande que no es necesario tener un plan de direccionamiento para un sitio que use diferentes valores de mascara de red. Es decir el calculo de la mascara de red para cada subred y el uso de mascaras de subred de longitud variable VLSM (Variable-Length Subset Masks) no se requieren por lo que en IPv6 la asignación de subredes (subnetting) es más simple que en IPv4.

3.4.4.3 Identificador de Interfaz

Este es el ultimo campo de la dirección IPv6, es un campo de 64 bits de longitud fija. Es de 64 bits de largo para acomodar el mapeo de direcciones MAC de 48 bits como las de Ethernet y el mapeo de direcciones MAC IEEE 1394 de 64 bits El identificador de interfase puede ser formado de las siguientes formas:

- **Derivación del identificador de la dirección MAC IEEE 802. Mapeo de una dirección MAC de 48 bits (IEEE 802) a una representación de 64 bits (EUI-64). Direcciones IEEE 802.**
  Los adaptadores de red de las tecnologías LAN como Ethernet, Token Ring, y FDDI usan una dirección de 48 bits llamada dirección IEEE 802, Fig. 3.4.4.3.1.

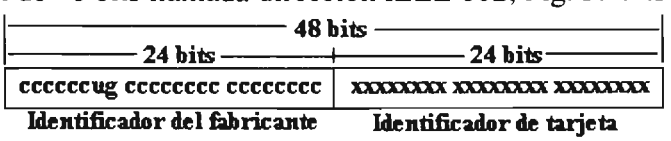


Fig. 3.4.4.3.1 Estructura de la dirección MAC IEEE802

Esta dirección consiste de un identificador del fabricante (manufacturer ID) de 24 bits asignado a cada uno de los fabricantes de adaptadores de red, y un identificador de tarjeta (board ID) de 24 bits asignado unívocamente a cada adaptador cuando se fabrican. Estos identificadores producen una dirección globalmente única también conocida como dirección física, dirección de hardware o dirección MAC (Media Access Control). Esta dirección tiene dos bits definidos que son:

El bit Universal/Local (U/L). En el primer byte de la dirección MAC el bit anterior al de mas bajo orden (ccccccug) es usado para indicar si la dirección es administrada localmente o universalmente. Si el bit U/L es puesto a 0 el IEEE (a través de la designación de un identificador de fabricante único) ha administrado la dirección. Si el bit U/L vale 1, la dirección es localmente administrada, en este caso el administrador de red ha anulado la dirección fabricada y especificado una dirección diferente.

El bit Individual/Grupo (I/G). El bit de mas bajo orden del primer byte de la dirección MAC indica si la dirección es una dirección individual (unicast) o una dirección de grupo (multicast). Cuando es puesto a 0, la dirección es una dirección unicast. Cuando es puesto a 1, la dirección es una dirección multicast.

Para una dirección de adaptador de red 802.x típica, los dos bits U/L y I/G valen 0, lo que significa que es una dirección MAC unicast, universalmente administrada.

Para fines de la autoconfiguración de direcciones y de la movilidad este identificador genera direcciones IPv6 únicas y universales en formato EUI-64 (Extended universal identifier) expandiendo la dirección física o MAC de la interfase LAN. En Ethernet, el método definido por el IEEE para determinar este identificador y que es generada de acuerdo al RFC 2464, es como muestra la Fig. 3.4.4.3.2:

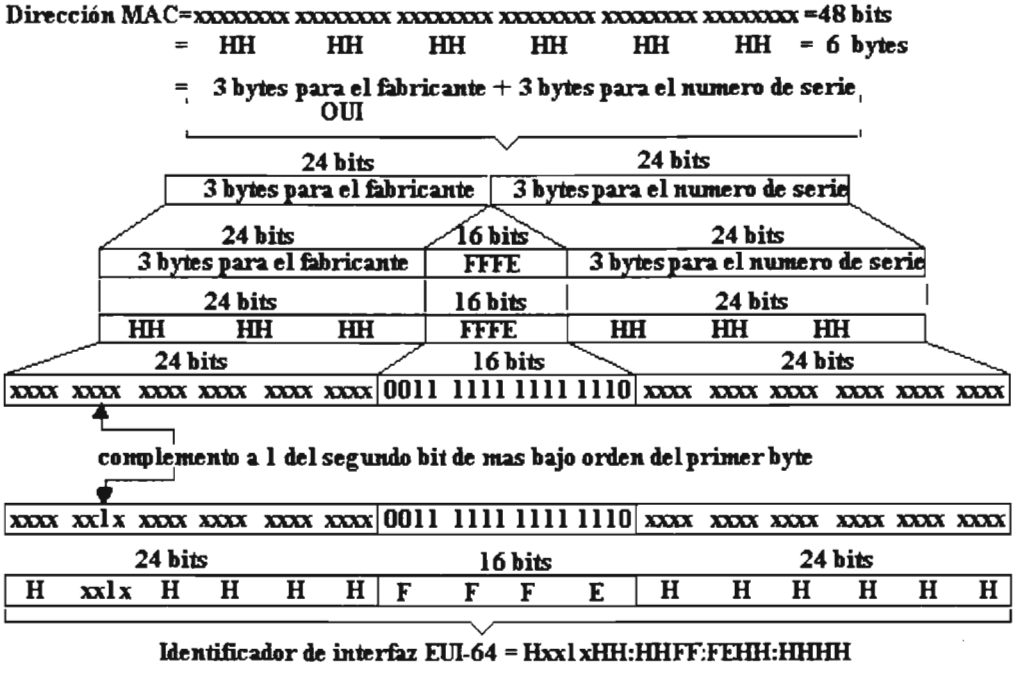


Fig. 3.4.4.3.2 Generación del identificador de interfaz en formato EUI-64 mediante el mapeo de la dirección MAC de 48 bits a IPv6

Hasta ahora las direcciones MAC eran de 48 bits, 24 bits asignados por el IEEE y conocidos como OUI (Organization Unique Identifier) y 24 bits seleccionados por el fabricante.
Para convertir una dirección IEEE 802 a identificador de interfaz de 64 bits, primero se debe mapear a un formato EUI-64 y después complementar el bit U/L.
Como se puede observar en la Fig. 3.4.4.3 el mapeo de la dirección MAC de 48 bits a 64 bits para generar el identificador de interfaz es realizado al insertar los dígitos hexadecimales FFFE entre los tres primeros bytes de la dirección Ethernet y los tres últimos bytes.
Posteriormente ya sea que se ejecute una función or-exclusiva del resultado con 0200:0000:0000:0000 o se toma el primer octeto de esta dirección MAC (primer octeto de izquierda a derecha), se convierte a binario y al segundo bit (bit Universal/local) de mas bajo orden del primer byte se le aplica el complemento a 1, es decir, si el bit U/L=1 es puesto a 0 y si vale 0 es puesto a 1. Se complementa el bit U/L para tener mayor compresibilidad de direcciones EUI-64 localmente administradas. (Cuando se complementa el bit U/L, agregar 0x2 al primer byte si la dirección EUI-64 es universalmente administrada, y restar 0x2 del primer byte si la dirección EUI-64 es localmente administrada).
Ya que las direcciones Ethernet son globalmente únicas, esto ayuda a generar una dirección IPv6 única.
Un ejemplo de este procedimiento es:
Si la dirección MAC es:
00-0b-cd-a9-52-8b
Entre el tercer octeto (cd) y el cuarto (a9) se inserta fffe: **00-0b-cd-ff-fe-a9-52-8b**
El segundo bit menos significativo del primer octeto (00) se complementa a 1, es decir, si el primer octeto es:
0x00=00000000
El complemento del segundo bit a 1 es: 00000010
Por lo tanto el primer octeto de la dirección MAC en notación hexadecimal ahora es 02:
Así el identificador de interfaz ahora es: **02-0b-cd-ff-fe-a9-52-8b.**
Agrupados en grupos de 4 octetos: 020b:cdff:fea9:528b.

- **Derivación del identificador de la dirección MAC de 64 bits. Mapeo de una dirección de EUI a IPv6**
  Direcciones IEEE EUI-64. La dirección IEEE EUI-64 es un nuevo estándar para el direccionamiento de interfaz de red, Fig. 3.4.4.3.3.

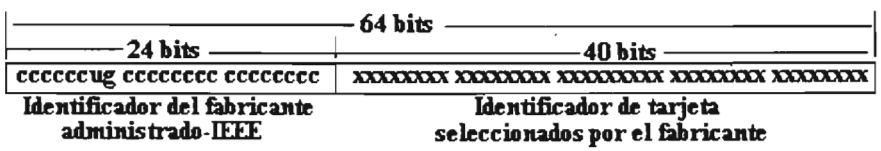


Fig. 3.4.4.3.3 Estructura de la dirección EUI-64

El identificador del fabricante sigue siendo de 24 bits, pero el identificador de extensión es de 40 bits, haciendo un espacio de dirección mucho mas largo para un fabricante de adaptadores de red. Usa los bits U/L e I/G en la misma forma que la dirección IEEE 802.

En este método cualquier compañía que haya recibido un OUI del IEEE puede usarlo para generar el nuevo identificador EUI-64. Para ello será suficiente usar el identificador del fabricante (OUI) como los primeros 24 bits y agregarle los últimos 40 bits seleccionados por el fabricante para sus productos, además de que nuevamente al penúltimo bit (bit Universal/Local) de izquierda a derecha del primer byte del OUI se complementa a 1, como muestra la Fig. 3.4.4.3.4.

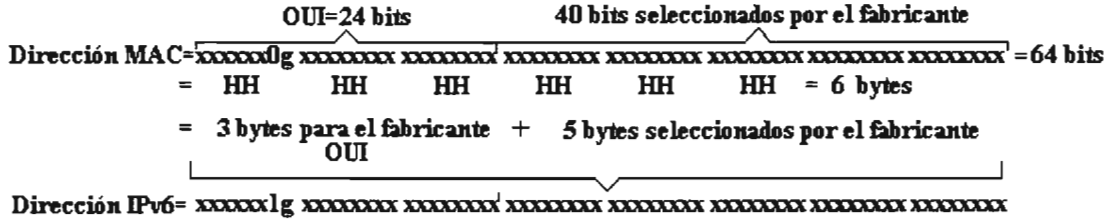


Fig. 3.4.4.3.4 Generación del identificador de interfaz en formato EUI-64 mediante el mapeo de la dirección EUI-64 a IPv6

Como el bit U/L se complementa cuando se convierte una dirección EUI-64 a un identificador de interfaz IPv6, el bit resultante en el identificador de interfaz tiene la interpretación opuesta del bit U/L definido por el IEEE. Si el séptimo bit del identificador de interfaz IPv6 es puesto a 0, es localmente administrado, si es puesto a 1 es universalmente administrado.

- El identificador de interfase también puede ser formado o asignado por medio de un servidor DHCPv6.
- Los 64 bits del identificador también pueden ser configurados manualmente.
- Temporalmente asignado. Un procedimiento pseudo aleatorio también puede autogenerar los 64 bits que componen al identificador de interfase para proporcionar cierto nivel de anonimato.

  Para conexiones por marcación (dial-up) al usuario se le asigna un prefijo de 64 bits cuando se conecta mediante mensajes de descubrimiento de router. Si el identificador de interfaz se basa en la dirección EUI-64 que se deriva de la dirección IEEE 802, se puede seguir el trafico de un nodo a pesar de que el prefijo cambie en cada conexión. Por lo que una derivación alternativa del identificador de interfaz IPv6 es aleatoriamente generada y cambia con el tiempo. El identificador de interfaz inicial es generado mediante técnicas de números aleatorios. Un nuevo identificador de interfaz es generado cada vez que el protocolo IPv6 es inicializado para sistemas IPv6 que no almacenan un historial. Para sistemas IPv6 que almacenan valores, cuando se inicia el protocolo IPv6 un nuevo identificador se crea de la siguiente forma:

  1. Recupera los valores almacenados y agrega el identificador basado en la dirección EUI-64.
  2. Calcula la clave de dispersión (hash) MD5 sobre la cantidad del paso 1. El calculo de la clave de dispersión MD5 producirá un valor de 128 bits.
  3. Almacena los 64 bits de mas bajo orden de la clave de dispersión MD5 calculado del paso 2 como el valor histórico para el siguiente calculo del identificador de interfaz.

4. Toma los 64 bits de mayor orden de la clave de dispersión MD5 calculado en el paso 2 y pone el séptimo bit a 0 que indica que es un identificador de interfaz administrado localmente. El resultado es el identificador de interfaz.

Esa dirección IPv6 resultante es conocida como dirección temporal. Estas direcciones son generadas para prefijos de dirección públicos que usan la autoconfiguración de dirección stateless. Las direcciones temporales son usadas por los valores más bajos de los siguientes tiempos de vida validos y preferidos:

- Tiempos de vida de la opción Información de prefijo del mensaje anunciamiento de router.
- Valores locales por default de 1 semana para el tiempo valido y 1 día para el tiempo preferido.

Después de que el tiempo de vida de la dirección temporal termina, un nuevo identificador de interfaz y una dirección temporal son generados.

➢ El identificador de interfaz puede estar basado en direcciones de capa de enlace o números seriales, o aleatoriamente generado cuando se configura una interfaz con el protocolo PPP y una dirección EUI-64 no esta disponible.

3.4.4.4 Tipos de direcciones IPv6

En IPv6 las direcciones se asignan a interfaces de red (no se asignan a nodos como en IPv4) y cada interfase posee y usa diferentes direcciones IPv6 simultáneamente. IPv6 divide las direcciones en tipos de forma análoga a como IPv4 las divide en clases.
En IPv6 se tienen tres tipos básicos de direcciones tipo anycast que se clasifican según se usen para identificar a un interfaz en concreto o a un grupo de interfaces. La distinción del tipo de dirección es en base a los bits de mayor peso (prefijo), se emplea un numero variable de bits para cada caso. Se tienen tres tipos de direcciones genéricas y bajo el ámbito de cada clase de direcciones se tienen uno o más tipos de direcciones:

- Direcciones anycast. Direcciones de agregación global, de sitio-local y enlace-local.
- Direcciones multicast. Direcciones asignadas y de nodo solicitado.
- Direcciones unicast. Direcciones de enlace-local, sitio-local, agregación global, direcciones compatible con IPv4, loopback, no especificadas.

3.4.4.4.1 Direcciones anycast (Monodistribución)

Anycasting es una técnica en la cual un nodo fuente manda un paquete al miembro más cercano de un grupo anycast.
Las direcciones anycast identifican a un conjunto de interfaces que pertenecen a diferentes nodos que comparten un prefijo (pertenecientes a diferentes nodos). Cuando un paquete se dirige a una dirección anycast el paquete se ruteara y se entregara solamente a la interfaz más cercana de las que forman parte del conjunto según lo determine la medida de la distancia (métrica) del protocolo de ruteo.
Las direcciones anycast son asignadas a partir de los prefjos unicast usando alguno de los formatos de dirección unicast definidos, por lo que las direcciones anycast son indistinguibles de las direcciones unicast, cuando una dirección unicast es asignada a mas de una interfaz se convierte en una dirección anycast. Este tipo de direcciones son en

realidad direcciones unicast que se encuentran asignadas a varias interfaces que necesitan ser configuradas de manera especial.
Para cualquier dirección anycast existe un prefijo de dirección mas largo P que identifica la región topológica en la cual todas las interfaces pertenecientes a esa dirección anycast residen. Dentro de esa región P cada miembro anycast debe ser anunciado como una entrada separada en el sistema de ruteo (ruta host); fuera de la región P, la dirección anycast debe ser agregada en los anunciamientos de ruteo para el prefijo P.
Debido a la falta de experiencia en el uso con este tipo de direcciones se tienen restricciones como:

- Una dirección anycast no debe ser usada como la dirección fuente de un paquete IPv6.
- La dirección anycast no debe ser asignada a un host IPv6, puede ser asignada solamente a un router IPv6.

El formato predefinido de una dirección anycast subred-router tiene el formato de la Fig. 3.4.4.4.1.1.

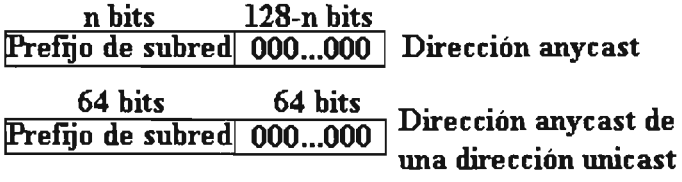


Fig. 3.4.4.4.1.1 Formato de una dirección anycast subred-router

- El prefijo de subred es el prefijo que identifica al enlace local
- La dirección anycast es sintáctica mente igual a la dirección unicast de una interfaz en el enlace excepto por que el identificador de interfase es puesto a cero.

La dirección anycast reservada se forma de los 64 bits de subred del prefijo unicast y los restantes 64 bits de mas bajo orden son puestos a cero. Esta dirección anycast reservada es también llamada dirección anycast subred-router. Todos los routers deben soportar estas direcciones en cada una de sus interfaces.
Los paquetes enviados a una dirección anycast subred-router serán entregados a un router en la subred.
Usos esperados de las direcciones anycast es la identificación del conjunto de routers pertenecientes a una organización que proporciona servicio de Internet, o la identificación del conjunto de routers conectados a una subred particular, o el conjunto de routers que proporcionan entradas en un dominio particular de ruteo.
Las direcciones anycast permiten a un nodo seleccionar cual de los distintos proveedores utilizar y se pueden aplicar para balancear el trafico en necesidades de alta disponibilidad.
Se pretende usar las direcciones anycast en aplicaciones donde un nodo necesita comunicarse con un router que pertenece a un conjunto de routers en una subred remota, como en la movilidad IP donde un host móvil necesita comunicarse con uno de los agentes móviles de su subred local. Cuando un nodo móvil esta lejos de su red local y desea descubrir la dirección IPv6 de su agente local, puede usar anycasting, el nodo móvil puede mandar un mensaje ICMPv6 de petición de descubrimiento de la dirección del agente local a la dirección anycast del agente móvil, el nodo debe esperar un mensaje ICMPv6 con la respuesta de descubrimiento de la dirección del agente local conteniendo una lista de agentes locales.

3.4.4.4.2 Direcciones multicast (Multidistribución):

Multicast es una técnica en la cual un nodo fuente manda un solo paquete a múltiples destinos simultáneamente.
Este tipo de direcciones identifica a un conjunto de interfaces de la red (pertenecientes a diferentes nodos), cuando un paquete se envía a una dirección multicast el paquete es entregado a todas las interfaces identificadas por esa dirección.
La idea principal de multicasting es tener una red eficiente que ahorre ancho de banda en los enlaces optimizando el numero de paquetes intercambiados entre nodos.
Multicasting usa rangos de direcciones, en IPv4 este rango es 224.0.0.0/3, en IPv6 es FF00::/8, como muestra la siguiente tabla:

Representación	Valor
Formato preferido	FF00:0000:0000:0000:0000:0000:0000:0000:/8
Formato comprimido	FF00:0:0:0:0:0:0:0/8=FF00::/8
Formato binario	1111 1111. Los 8 bits de mayor orden son puestos a 1.

Las direcciones de broadcast no se implementan en esta versión del protocolo, el broadcast desaparece debido a que se puede realizar ahora mediante el uso de las direcciones de multicast. El formato de las direcciones multicast es el mostrado en la Fig. 3.4.4.4.2.1

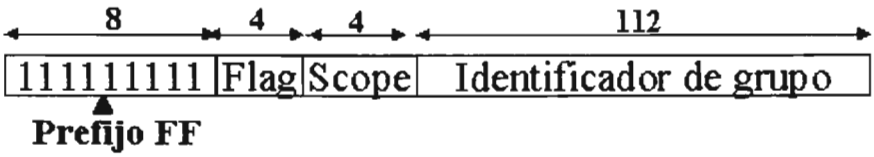


Fig. 3.4.4.4.2.1 Formato de las direcciones Multicast

Los campos de esta dirección son:

- FD: Este campo de 8 bits con valor 11111111 identifica la dirección como una dirección multicast, mediante el prefijo FF00::/8.
- Flags: Campo de 4 bits que indica el tiempo de vida de las direcciones multicast, cuando los bits de las banderas de mayor orden están reservados, y deben ser inicializados a cero. El campo FLGS esta fijado en 000T donde 000 esta reservado y el valor de T es:
  T=0 (0000) indica una dirección multicast asignada permanentemente (bien conocida) por la autoridad de numeración Global de Internet IANA.
  T=1 (0001) indica una dirección multicast transitoria no asignada permanentemente, es decir, es una dirección de transito o temporal.
- SCOPE: Es un valor que indica el ámbito multicast usado para limitar el alcance del grupo multicast. Este valor es obligatorio para limitar la transmisión de paquete multicast a determinadas áreas o sectores de la red. Sus valores se listan en la tabla 3.4.4.4.2.1:

Valor Hexadecimal	Reservado	Rep. Binaria
0	Reservado	0000
1	Ámbito de nodo local o interfaz local	0001
2	Ámbito de enlace local (link-local)	0010
3	Ámbito de subred local	0011
4	Ámbito de administración local	0100
5	Ámbito local al sitio (site-local)	0101
6	Sin asignar	0110
7	Sin asignar	0111
8	Ámbito de organización local	1000
9	Sin asignar	1001
A	Sin asignar	1010
B	Ámbito de comunidad local	1011
C	Sin asignar	1100
D	Sin asignar	1101
E	Ámbito global	1110
F	Reservado	1111

Tabla 3.4.4.4.2.1 Valores del campo ámbito de la dirección multicast

- Identificador de grupo: Identifica al grupo multicast, ya sea permanente o transitorio dentro de un ámbito dado.

Las direcciones multicast pueden ser de ámbito fijo o de alcance variable. Las de alcance fijo están permanentemente asignadas y son validas sobre un valor de alcance especificado. Las de ámbito variable están permanentemente asignadas y son validas sobre todos los rangos de alcance, los cuales son identificados por una X en el campo ámbito (scope) que significa cualquier valor de ámbito legal. Las direcciones multicast que son diferentes en alcance, representan diferentes grupos. Los nodos deben unirse a cada grupo individualmente.
Algunas direcciones de multicast (prefijo FF00::/8), dentro del rango reservado FF00:: a FF0F:: se han asignado para identificar funciones especificas o especiales como se muestra en la tabla 3.4.4.4.2.2:

Direcciones multicast de ámbito fijo	
Ámbito nodo local	
FF01:0:0:0:0:0:0:1 = FF01::1	Dirección multicast a todos los nodos dentro del ámbito nodo-local (solo ese host).
FF01:0:0:0:0:0:0:2 = FF01::2	Dirección multicast a todos los routers dentro del ambito nodo-local.
Ámbito enlace-local	
FF02:0:0:0:0:0:0:1 = FF02::1	Es la dirección multicast a todos los nodos en la red o enlace local.
FF02:0:0:0:0:0:0:2 = FF02::2	Es la dirección multicast a todos los routers en la red o enlace local.
FF02:0:0:0:0:0:0:3 = FF02::3	Dirección multicast sin asignar.
FF02:0:0:0:0:0:0:4 = FF02::4	Dirección multicast routers DVMRP.
FF02:0:0:0:0:0:0:5 = FF02::5	Dirección multicast ruteadores OSPFIGP.
FF02:0:0:0:0:0:0:6 = FF02::6	Dirección multicast routers designados OSPFIGP.
FF02:0:0:0:0:0:0:7 = FF02::7	Dirección multicast routers ST.
FF02:0:0:0:0:0:0:8 = FF02::8	Dirección multicast hosts ST.
FF02:0:0:0:0:0:0:9 = FF02::9	Dirección multicast routers RIP.
FF02:0:0:0:0:0:0:A = FF02::A	Dirección multicast routers EIGRP.
FF02:0:0:0:0:0:0:B = FF02::B	Dirección multicast agentes móviles.
FF02:0:0:0:0:0:0:C = FF02::C	Dirección multicast SSDP.
FF02:0:0:0:0:0:0:D = FF02::D	Dirección multicast todos los routers PIM.
FF02:0:0:0:0:0:0:E = FF02::E	Dirección multicast encapsulación-RSVP.
FF02:0:0:0:0:0:0:16 = FF02::16	Dirección multicast todos los routers capaces-MLDv2.
FF02:0:0:0:0:0:0:6A = FF02::6A	Dirección multicast todos los snoopers.
FF02:0:0:0:0:0:1:1 = FF02::1:1	Dirección multicast nombre del enlace.
FF02:0:0:0:0:0:1:2 = FF02::1:2	Dirección multicast todos los agentes DHCP.
FF02:0:0:0:0:0:1:3 = FF02::1:3	Dirección multicast de enlace local para la resolución de nombres.
FF02:0:0:0:0:0:1:4 = FF02::1:4	Dirección multicast de anunciamiento DTCP.
FF02:0:0:0:0:1:FFXX:XXXX= FF02::1:FFXX:XXXX	Dirección multicast de nodo solicitado, donde XX:XXXX son los últimos 24 bits de la dirección IPv6 de nodo solicitado ya sea unicast o anycast.
Ambito sitio-local	
FF05:0:0:0:0:0:0:2 = FF05::2	Dirección multicast a todos los routers en el sitio local.
FF05:0:0:0:0:0:1:3 = FF05::1:3	Dirección multicast todos los servidores DHCP.
FF05:0:0:0:0:0:1:4 = FF05::1:4	Multicast todos los relays DHCP (desaprobada).

Tabla 3.4.4.4.2.2 Asignación de direcciones multicast

- **Dirección Multicast de nodo seleccionado**

La dirección multicast de nodo seleccionado es un tipo especial de dirección multicast. Por cada dirección unicast y anycast configurada sobre una interfaz de un nodo o de un router, una dirección multicast de nodo solicitado es automáticamente habilitada, esta dirección esta limitada al enlace local. Este tipo de dirección es usada para dos propósitos:

- Reemplazo del protocolo ARP de IPv4. Ya que ARP no se usa en IPv6, la dirección multicast de nodo solicitado se usa por los nodos y routers para conocer las direcciones de capa de enlace de nodos y routers vecinos en el mismo enlace local. El conocimiento de la dirección de capa de enlace es obligatorio para poder hacer la entrega de paquetes IPv6 en tramas de capa de enlace.
- Detección de dirección duplicada (DAD). Este mecanismo de detección es parte del protocolo de descubrimiento de vecinos. Permite a un nodo verificar sí una dirección ya esta en uso en el enlace local antes de usarla para la configuración de dirección IPv6 mediante un mecanismo stateless. La dirección de nodo solicitado se usa para checar en el enlace local que la dirección unicast o anycast no este configurada en otro nodo.

La dirección de nodo solicitado se define por un prefijo como muestra la siguiente tabla:

Representación	Valor
Formato preferido	FF02:0000:0000:0000:0000:0001:FF00:0000/104
Formato comprimido	FF02::1:FF00:000/104

Como podemos ver la dirección multicast de nodo solicitado consiste de prefijo FF02::1:FF00:000/104 y de los 24 bits de mas bajo orden de una dirección unicast o anycast, como muestra la Fig. 3.4.4.4.2.2

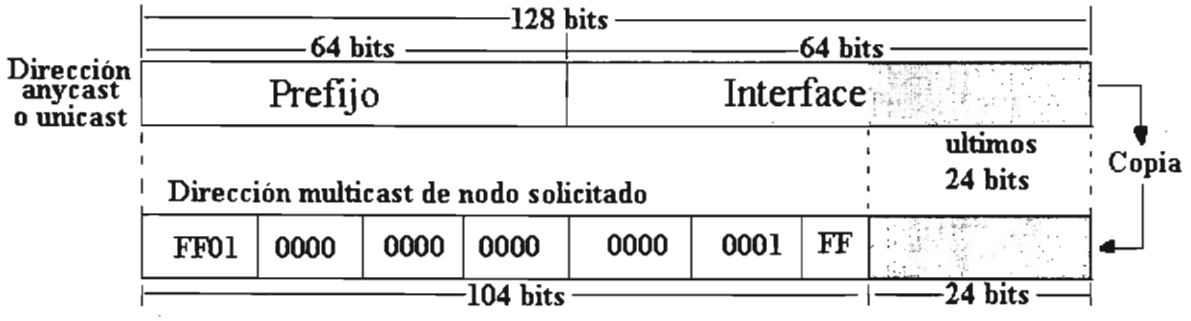


Fig. 3.4.4.4.2.2 Dirección multicast de nodo solicitado.

Como se observa en la Fig. 3.4.4.4.3 los 24 bits de mas bajo orden de una dirección anycast o unicast se agregan al prefijo FF02::1:FF.

Los nodos IPv6 (hosts o routers) deben unirse a los siguientes grupos multicast:

- Grupo multicast de todos los nodos FF02:0:0:0:0:0:0:1 (en el ámbito de enlace local)
- Grupo multicast de nodo solicitado FF02:0:0:0:0:FF00:0000/104 para cada una de sus direcciones unicast y anycast asignadas.
- Todos los routers se deben unir al grupo multicast de todos los routers FF02:0:0:0:0:0:0:2 (en el ámbito de enlace local).

Algunas direcciones multicast de ámbito variable se muestran en la tabla 3.4.4.4.2.3:

Direcciones multicast de ámbito variable	
FF0X:0:0:0:0:0:0:0 = FF0X::	Dirección multicast reservada.
FF0X:0:0:0:0:0:0:C = FF0X::C	Multicast SSDP.
FF0X:0:0:0:0:0:0:100 = FF0X::100	Grupo multicast de administradores VMTP.
FF0X:0:0:0:0:0:0:101 = FF0X::101	Protocolo de tiempo de red NTP.
FF0X:0:0:0:0:0:0:100 = FF0X::106	Servidor de servicio de nombre.
FF0X:0:0:0:0:0:0:108 = FF0X::108	Servicio de información SUN NIS+.
FF0X:0:0:0:0:0:0:109 = FF0X::109	Protocolo de transporte multicast.
FF0X:0:0:0:0:0:0:10B = FF0X::10B	IETF-1-audio.
FF0X:0:0:0:0:0:0:114 = FF0X::114	Cualquier experimento privado.
FF0X:0:0:0:0:0:0:115 = FF0X::115	DVMRP sobre MOSPF.
FF0X:0:0:0:0:0:0:120 = FF0X::120	mtrace.
FF0X:0:0:0:0:0:0:121 = FF0X::121	RSVP-encap-1.
FF0X:0:0:0:0:0:0:127 = FF0X::127	anunciamiento-cisco-rp.
FF0X:0:0:0:0:0:0:129 = FF0X::129	Gatekeeper.
FF0X:0:0:0:0:0:0:300 = FF0X::300	Mbus/IPv6.
FF0X::2:0000-FF0x::2:7FFD	Llamadas de conferencia multimedia
FF0X:0:0:0:0:0:2:7FFE=FF0X::2:7FFE	Anunciamientos SAPv1
FF0X::2:8000-FF0X::2:FFFF	Asignaciones dinámicas SAP

Tabla 3.4.4.4.2.3 Direcciones multicast de abito variable

En el ambiente Ethernet la dirección multicast IPv6 se relacionan con las direcciones ethernet agregando los últimos 32 bits de la dirección multicast al prefijo 33:33: para multicast ethernet. El nodo que transmite un paquete multicast IPv6 usa esta nueva dirección ethernet multicast para alcanzar el destino en el enlace local, como se observa en el siguiente extracto de un paquete capturado:

Ethernet II, Src: 00:0b:cd:a9:52:8b, Dst: **33:33:ff:55:2f:41**

Destination: **33:33:ff:55:2f:41** (IPv6-Neighbor-Discovery_ff:55:2f:41)

Source: 00:0b:cd:a9:52:8b (CompaqHp_a9:52:8b)

Type: IPv6 (0x86dd)

La comunicación por multicast es un servicio no orientado a conexión. Los grupos multicast no tienen ninguna restricción en cuanto al numero de grupos, ni tampoco tienen restricción en cuanto al numero de miembros de cada grupo.

La dirección destino en la transmisión multicast es un grupo de direcciones, donde el nodo que transmite hacia una dirección multicast no necesariamente debe pertenecer al grupo.

El esquema de direccionamiento IPv6 esta diseñado para soportar millones de direcciones de grupo multicast.

Ipv6 usa mucho las direcciones multicast en los mecanismos para reemplazar a ARP, en el anunciamiento de prefijos, detección de direcciones duplicadas (DAD) y renumeración de prefijos. Los nodos IPv6 conocen sus nodos vecinos y router vecinos mandando y escuchando paquetes multicast en el enlace local, a diferencia de los nos IPv4 que usan ARP.

La comunicación multicast se puede aplicar en sistemas distribuidos, video en demanda, difusión de radio y televisión, conferencia multipunto de voz o video, juegos de red.

3.4.4.4.3 Direcciones unicast (Unidistribución):

Unicast es la técnica en la cual un nodo fuente manda un solo paquete a un solo destino.
Una dirección unicast es la dirección de una sola interfase. Identifican y por lo tanto son dirigidas a un único interfaz individual de la red, estas direcciones se dirigen de un host a otro host. Los paquetes que se envían a una dirección unicast son entregados solamente a la interfaz identificada con esa dirección.
Los nodos IPv6 pueden tener poco conocimiento de la estructura interna de una dirección IPv6, por lo que en el caso más simple pueden considerar la dirección IPv6 como una cadena de 128 bits, Fig. 3.4.4.4.3.1:

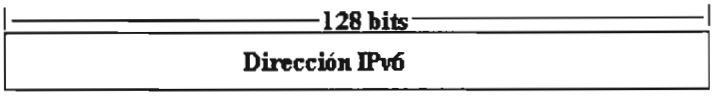


Fig. 3.4.4.4.3.1 Dirección IPv6 como una cadena de 128 bits

Con una mejor visión los nodos pueden ver la dirección IPv6 estructurada en dos partes viendo al prefijo como identificador de la subred, Fig. 3.4.4.4.3.2:

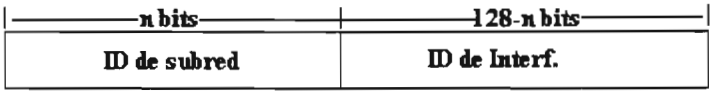


Fig. 3.4.4.4.3.2 Dirección IPv6 y prefijo.

En las redes LAN la dirección unicast permite identificar el nodo dentro de la subred de su dirección MAC de 48 bits en formato EUI-64 de 64 bits, Fig. 3.4.4.4.3.3:

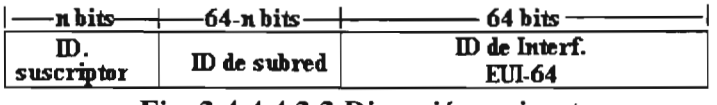


Fig. 3.4.4.4.3.3 Dirección unicast

El identificador de suscriptor identifica el conjunto de direcciones asignadas a una organización dada. El identificador de subred divide este conjunto en subredes, el identificador de interfase identifica la interfase dentro de la subred.
Si la organización es grande, un solo nivel de jerarquía puede no ser útil, por lo que se pueden usar mas niveles de jerarquía, Fig. 3.4.4.4.3.4:

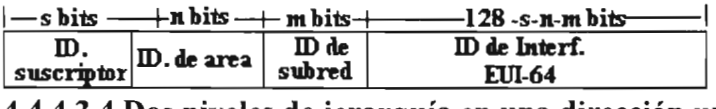


Fig. 3.4.4.4.3.4 Dos niveles de jerarquía en una dirección unicast

En este caso se usa un identificador de interfase menos a 64 bits para dejar mas espacio a los campos identificador de área y de subred.

3.4.4.4.3.1 Tipos de direcciones unicast

Las direcciones unicast se subdividen a su vez en varios tipos dependiendo del ámbito de funcionamiento:

- Direcciones unicast de ámbito local al enlace (link-local).
  IPv6 maneja direcciones unicast limitadas, que son usadas solamente en un contexto restringido. Estas direcciones tienen el prefijo FE80::/10 = **1111 1110 10**00 0000 o FE80::<Interface ID>. Son de uso limitado a la red local y automáticamente configuradas en todos los nodos usando identificadores de interfaz. Estas direcciones se usan para descubrimiento de vecinos y descubrimiento de routers y se pueden usar como una red local IPv6 no ruteada globalmente.
- Direcciones unicast de ámbito local al sitio (site-local).
  Estas direcciones tienen el prefijo FEC0::/10 = **1111 1110 11**00 0000. Estas direcciones se limitan a direccionar un sitio local u organización entera sin direcciones globales. Los ruteadores no deben reenviar estas direcciones. Se configuran usando un identificador de interfase y un identificador de subred de 16 bits en la forma FEC0::<subred ID>:<interface ID>.
- Direcciones mapeadas a IPv4.
  Son direcciones del tipo ::FFFF:w.x.y.z
- Direcciones compatibles con IPv4 o con direcciones IPv4 insertadas.
  Este es un formato especial del tipo ::w.x.y.z que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.
- Direcciones unicast globales de agregación.
  Son direcciones globalmente unicas que pueden ser usadas en cualquier lugar. Estas direcciones tienen el prefijo 2000::/3 = **001**0 0000 0000 0000.

Estas son las direcciones unicast usadas actualmente, existen otros tipos que ya no se usan:

- Direcciones unicast de interconexión-neutral.
- Direcciones unicast globales basadas en el proveedor
- Globales basadas en la geografía (prácticamente sin uso por los inconvenientes que representan para la administración de su ruteo), a nivel NSAP, a nivel jerárquico IPX
- De maquinas IP-only

3.4.4.4.3.2 Direcciones de uso local al enlace (link-local).

Cuando la pila de IPv6 es habilitada en un nodo, una dirección de enlace local es automáticamente asignada a cada interfaz cuando el nodo reinicia. El formato de las direcciones locales al enlace es mostrado en la Fig. 3.4.4.4.3.2.1.

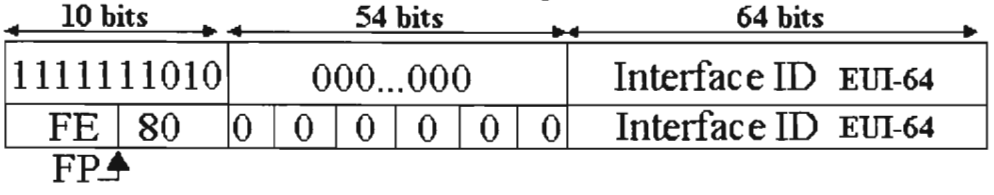


Fig. 3.4.4.4.3.2.1 Formato de las direcciones locales al enlace (link-local)

El prefijo de estas direcciones es de 10 bits y se representa como FE80::<Interface ID>/10. El identificador de Interfaz en formato EUI-64 (Extended Unique Identifier 64) es agregado a los 64 bits de mas bajo orden de la dirección. Los bits 11 hasta 64 son puestos a cero. Así la forma de representar las direcciones de enlace-local se muestra en la siguiente tabla:

Representación	Valor
Formato preferido	FE80:0000: 0000: 0000: 0000: 0000: 0000: 0000/10
Formato comprimido	FE80:0:0:0:0:0:0:0/10=FE80::/10
Formato binario	1111 1110 10. Valor de los 10 bits de mayor orden

Estas direcciones están diseñadas para usarse en un enlace único. Las direcciones de enlace local son validas solamente para un enlace especifico de LAN por lo que solamente se usan entre nodos conectados en el mismo enlace local., donde no hay un nodo de router en la red (funcionan como las direcciones privadas en IPv4), son usadas para efectos de autoconfiguración y funciones de descubrimiento de vecino. Este tipo de direcciones son usadas por los nodos para comunicarse con su router por default independientemente de la dirección unicast de agregación global. Estas direcciones no son ruteables fuera de su ámbito local al enlace, es decir no deben ser ruteadas entre subredes dentro de un sitio.
Las direcciones de enlace local son permanecen sin cambio en nodos y routers aunque se dé un proceso de renumeración, la que cambia es la dirección unicast de agregación global únicamente.

3.4.4.4.3.3 Direcciones de uso local al sitio (site-local).

La dirección local al sitio es otra dirección unicast limitada para ser usada solamente dentro de un sitio, tienen el formato de la Fig. 3.4.4.4.3.1.

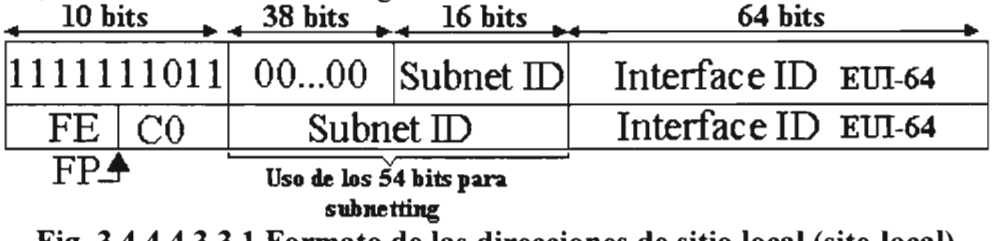


Fig. 3.4.4.4.3.3.1 Formato de las direcciones de sitio local (site-local)

La dirección consiste de un prefijo de 10 bits FEC0::/10, un campo de 54 bits llamado subnet ID y los 64 bits de mas bajo orden que forman el identificador de interfaz en formato EUI-64.
El campo de 54 bits es usado para subneteo del sitio permitiendo crear hasta 2^{54} diferentes subred IPv6. Inicialmente el identificador de subred era de 16 bits permitiendo crear hasta 65,536 subredes IPv6 diferentes. La forma de representar estas direcciones es:

Representación	Valor
Formato preferido	FEC0:0000: 0000: 0000: 0000: 0000: 0000: 0000/10
Formato comprimido	FEC0:0:0:0:0:0:0:0/10=FEC0::/10
Formato binario	1111 1110 11. Valor de los 10 bits de mayor orden

Estas direcciones no son habilitadas por default por lo que deben ser asignadas manualmente. Este tipo de direcciones son validas solamente dentro de una organización

particular no en la red de Internet, reemplazan a las direcciones privadas IPv4 (10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16). Pueden ser usadas por organizaciones que no han recibido espacio unicast de agregación global y pueden asignar un prefijo de sitio local a cualquier nodo y router dentro del sitio.
Las direcciones de site-local son usadas para diseñar el direccionamiento interno de un sitio para la interconexión de interfaces sin la necesidad de un prefijo global. Permiten crear subredes con ellas mediante el identificador de subred de 16 bits, que se ha alargado a 54 bits. Los routers no deben reenviar paquetes con dirección este tipo de direcciones fuente o destino fuera del ámbito del sitio local. El prefijo de estas direcciones es de 10 bits y se presenta como FEC0::<Subnet ID><Interface ID>/10. Este tipo de direcciones se pueden usar en impresoras, servidores de Intranet, switches, gateways, access points, también servidores y routers que solo deben ser alcanzados internamente para propósitos de administración.

- **Direcciones Unicast basadas en proveedor:**

Estas direcciones son usadas para comunicación global, su funcionamiento es semejante al que tiene las direcciones IPv4 con CIDR. El formato de estas direcciones es el mostrado en la siguiente figura:

3 bits	n bits	m bits	o bits	p bits	o-p bits
FD 010	Registry ID	Provider ID	Suscriber ID	Subnet ID	Interface ID

Los campos de este formato de dirección son:

FD: El campo FD de tres bits con valor 010 identifica la dirección como proveedor.
Registry ID: Identifica al registro de dirección de Internet que asigna identificadores a los proveedores de servicios de Internet.
Provider ID: Es el identificador (asignado por el Registry ID) del proveedor de servicios de Internet que asigna porciones del espacio de dirección a los suscriptores.
Suscriber ID: Este campo distingue entre varios suscriptores conectados al proveedor de servicios de Internet.
Subnet ID: Este campo identifica un enlace físico especifico.
Interface ID: El identificador de interfase identifica una sola interfaz entre el grupo de interfaces identificado por el prefijo de subred.

Direccionamiento IPv6 a IPv4

Las direcciones IPv6 que se han de mapear a IPv4 se representan mejor como un prefijo IPv6 de 96 bits seguido de una dirección IPv4 en formato decimal separado por puntos. De esta forma tenemos dos tipos de direcciones IPv6 a IPv4 definidas.

3.4.4.4.3.4 Direcciones mapeadas a IPv4:

Es una dirección unicast IPv6 que representa la dirección IPv4 de un nodo IPv4-only, esta dirección se puede mapear unívocamente al espacio IPv4. Tienen el prefijo 0:0:0:0:0:FFFF, por ejemplo, 0:0:0:0:0:FFFF:192.0.0.24=::FFFF:192.0.0.4, su formato se muestra en la Fig. 3.4.4.4.3.4.1:

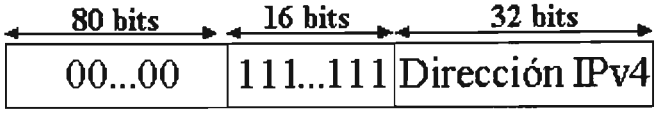


Fig. 3.4.4.4.3.4.1 Formato de la dirección IPv6 mapeada a IPv4

3.4.4.4.3.5 Direcciones compatibles con IPv4:

Es una dirección unicast IPv6 que transporta una dirección IPv4 en sus 32 bits de mas bajo orden, el prefijo es 0:0:0:0:0:0, por ejemplo, 0:0:0:0:0:0:192.0.0.24=::192.0.0.24, su formato es mostrado en la Fig. 3.4.4.4.3.5.1.

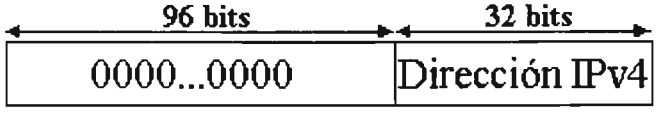


Fig. 3.4.4.4.3.5.1 Formato de la dirección IPv6 compatible con direcciones IPv4

Tanto las direcciones compatibles con IPv4 como mapeadas a IPv4 utilizan el mismo espacio de direcciones. El prefijo solo indica si el nodo soporta o no IPv6.

3.4.4.4.3.6 Direcciones unicast globales de agregación:

Las direcciones unicast de agregación global son direcciones IPv6 usadas para el trafico IPv6 genérico sobre el Internet IPv6.
Las direcciones unicast globales IPv6 son el equivalente de las direcciones unicast globales IPv4 usadas para la comunicación sobre el Internet IPv4.
Este tipo de direcciones son la parte más importante de la arquitectura de direccionamiento IPv6.
La estructura de las direcciones unicast de agregación global cumple con el objetivo principal de IPv6 que es el tener un plan de direccionamiento global consistente y escalable de direccionamiento.
El actual direccionamiento de IPv6 se conoce como direccionamiento unicast de agregación global, que permite tener en una estructura jerárquica de agregación de los prefijos de ruteo a base de mascaras de bits adyacentes como lo hace CIDR para IPv4, de este esquema de direccionamiento surge la estructura de las direcciones unicast de agregación global. Esta estricta agregación de los prefijos de ruteo limita el tamaño de la tabla de ruteo del Internet global
El concepto de agregación (aggregatable) es indispensable para una mejor organización jerárquica del ruteo en las redes globales. Este formato de direcciones soporta el tipo de agregación basado en proveedores (provider based) y el basado en intercambios (exchange based) la combinación de ambos permite un ruteo más eficiente.
La estructura de las direcciones unicast globales permite la agregación de prefijos de ruteo que limitan el número de entradas de la tabla de ruteo en la tabla de ruteo global. Las direcciones unicast globales son agregadas hacia arriba a través de las organizaciones y eventualmente a los ISPs.
En estas direcciones los 64 bits mas altos identifican la red y los 64 más bajos identifican el nodo.

Las direcciones unicast globales de agregación son identificadas por el prefijo del formato (FP) 001=2000, estas direcciones equivalen a las direcciones IPv4 publicas y son globalmente ruteables. El valor de este prefijo se debe a que la IANA asigno un rango de prefijo de dirección IPv6 del espacio completo de direccionamiento IPv6 para las direcciones unicast de agregación global

El espacio de dirección unicast global asignable se define como el bloque de dirección definido por el prefijo 2000::/3, como muestra la siguiente tabla:

Representación	Valor
Rango	2xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:/3
Primer dirección	2000:0000:0000:0000:0000:0000:0000:0000
Ultima dirección	3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Formato binario	001. Valor de los 3 bits de mayor orden.

Tres son los niveles de jerarquía del plan de direccionamiento IPv6:

1. Topología pública (public topology). Formada por el conjunto de proveedores de servicios y puntos de interconexión (exchanges) que proveen servicios públicos de transito en Internet. Este nivel consta de 48 bits.
2. Topología de sitio (Site Topology). Esta topología es local a un sitio especifico u organización que no provee servicio publico a nodos fuera del sitio. Básicamente con este nivel de 16 bits se identifican las redes en ámbitos privados o locales.
3. Identificador de Interfaz (Interface Identifier). Este identificador es un numero único en el segmento local de LAN, es de 64 bits y es generado automáticamente, identifica a las interfaces en los enlaces.

De esta forma las direcciones unicast de agregación global (Global Aggregate Unicast addresses) derivadas del esquema de direccionamiento de agregación global tienen el formato mostrado en la Fig. 3.4.4.4.3.6.1

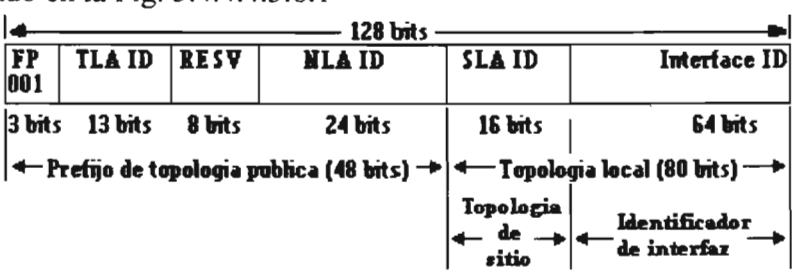


Fig. 3.4.4.4.3.6.1 Formato de la Dirección Unicast de Agregación Global (Global Aggregatable Unicast Addresses)

Podemos ver claramente en la Fig. 3.4.4.4.3.6.1 la separación de los tres niveles de jerarquía de la dirección unicast de agregación global.

Campos de la jerarquía, topología publica de la dirección unicast de agregación global.

En la Fig. 3.4.4.4.3.6.2 se observa que la topología publica a su vez se subdivide en cuatro campos.

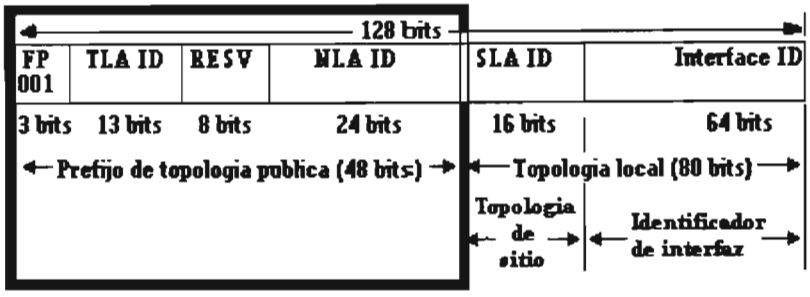


Fig. 3.4.4.4.3.6.2 Campos de la topología publica de una dirección unicast de agregación global.

Estos campos son:

- **Prefijo de formato (Format Prefix FP):**
  Se utiliza como identificador de agregación para direcciones unicast globales de agregación, se compone de tres bits con valor de 0010 que en la representación de prefijo tiene la forma 2::/3.

- **Top-level Aggregation Identifier (TLA ID):**
  Identificador de Agregación de alto nivel (Proveedor primario), este campo identifica el nivel superior en la jerarquía de ruteo.
  Es un identificador de los grandes proveedores internacionales. Un agregador de alto nivel TLA (algunas veces referidos como proveedores Tier-1) es un proveedor de red que esta situado en el máximo nivel de agregación del trafico de Internet, estos proveedores forman el núcleo del backbone de Internet. Estos TLA proporcionan el transporte de alta velocidad que mueve los paquetes de un aparte de global a otra, ya que sus backbones se componen de dispositivos de ruteo rápidos, altamente sofisticados y sus núcleos manejan las rutas de Internet completas. A estos proveedores se les asigna un bloque TLA o bloque de direcciones globalmente ruteables y a su vez ellos delegan parte de esos bloques a sus clientes.
  La IANA administra los TLA y asigna pequeños bloques de TLA ID a los registros de Internet IPv6 locales, que a su vez asignan TLAs individuales a los grandes ISPs de larga distancia. Este campo tiene una longitud de 13 bits que sumados a los 3 del campo FP originan un prefijo de 16 bits de longitud /16. Permite mas de 8000 niveles de Proveedores de servicios de Internet. Las direcciones son asignadas desde el proveedor por lo que al cambiar de proveedor se tiene que realizar una renumeración de hosts, routers y sitios que han sido incluidos en el protocolo IPv6.

Los routers situados en este nivel (nivel mas alto de la jerarquía de ruteo) no tienen una ruta por default, solo tienen en la tabla de ruteo una entrada con prefijo de 16 bits para cada TLA ID activo y tendrán entradas adicionales que proporcionaran información de ruteo del TLA ID en el que se encuentran. El numero de entradas que se tiene están pensadas para minimizar la tabla de ruteo. Soporta 8192 (2^{13}) identificadores TLA, este numero se puede incrementar usando el numero de bits del campo reservado o usando este formato para prefijos de formato adicionales.

- **Reservado (RESV):**
  Este campo de 8 bits de longitud esta reservado para uso futuro y debe tener un valor cero. Este campo permite un crecimiento futuro de los campos TLA ID o NLA ID.

- **Next Level Aggregation Identifier (NLA ID):**
  El identificador de agregación de siguiente nivel es usado por las organizaciones a las que se les asigno parte de un bloque TLA para crear una estructura jerárquica de direccionamiento, de acuerdo a su propia red y para identificar los sitios (los ISPs o proveedores de servicios de red Tier-2), organizaciones u operadores medianos que dependen del TLA e intercambian su trafico en un punto de interconexión TLA. Un NLA puede ser desde una pequeña organización con una conexión TLA hasta un gran proveedor regional con muchas conexiones TLA hacia arriba de la jerarquía (upstream). Un NLA recibe de su upstream TLA un NLA ID y a su vez lo divide en bloques que serán delegados a sus clientes.
  La longitud de este campo es de 24 bits que sumado a los 24 de los tres campos anteriores forma un prefijo de longitud /48=3+13+8+24, prefijos de 48 bits son asignados a los sitios de las organizaciones que se conectan al Internet IPv6. Cada organización puede manejar su NLA asignado de modo que reserve una porción para un nuevo NLA1 y crear así una jerarquía de direccionamiento apropiada a su red. El resto de los bits se utilizan para los sitios a los cuales desea dar servicio. Por ejemplo de los 24 bits se pueden usar n para crear un siguiente nivel NLA1 y los restantes 24-n bits para los sitios:

n bits	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interface ID

Las organizaciones a las que se les asigna un TLA ID tienen 24 bits para el NLA ID, esto permite a cada organización proporcionar servicio a aproximadamente tantas organizaciones como el numero total de direcciones IPv4 soportadas actualmente.
Las organizaciones que reciben un TLA ID pueden soportar varios NLA ID en su propio espacio de Site ID. Igualmente las organizaciones que reciben un NLA ID pueden usar su Site ID para soportar otros NLA ID, esto puede ver en forma general en el esquema de la Fig. 3.4.4.4.3.6.3

n bits	24-n bits			16	64 bits
NLA1	Site ID			SLA ID	Interface ID
	M	24-n-m		16	64 bits
	NLA2	Site ID		SLA ID	Interface ID
		o	24-n-m-o	16	64 bits
		NLA3	Site ID	SLA ID	Interface ID

Fig. 3.4.4.4.3.6.3 Esquema de jerarquización de los niveles de agregación NLA ID

Campos de la jerarquía, topología local o privada de la dirección unicast de agregación global.
En la Fig. 3.4.4.4.3.6.4 se observa que la topología local a su vez se subdivide en dos campos.

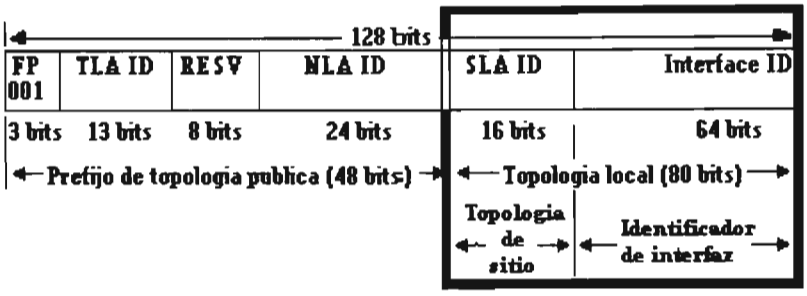


Fig. 3.4.4.4.3.6.4 Campos de la topología local de una dirección unicast de agregación global.

Estos campos son:

- **Identificador de agregación a nivel de sitio SLA ID (Site-Level Aggregation Identifier-tu sitio):**
  Un identificador de agregador a nivel de sitio describe a una entidad que no tiene clientes hacia debajo de la jerarquía (downstream) que sean ISPs. Un SLA puede ser un negocio grande o pequeño, un IPS pequeño que no delega espacios de dirección.
  Este identificador es un numero de subred de 16 bits de longitud que se asocia a un sitio que obtiene una asignación de dirección con prefijo de 64 bits (/48) que es la suma de 3+13+32+16, el cual es mucho más grande que una red de clase A en una red IPv4. Es usado por organizaciones finales para crear su propia jerarquía local de direccionamiento e identificar subredes. Es análogo al concepto de subred de IPv4 con la diferencia de que cada organización tiene un numero mayor de subredes.
  Este campo soporta 65355 (2^{16}) subredes individuales.
  El manejo del SLA ID depende de cada organización. El numero de subredes soportadas debería satisfacer las necesidades, excepto para organizaciones muy grandes, las cuales podrán solicitar otros identificadores SLA para tener subredes adicionales.

Al igual que el campo NLA, este campo SLA puede dividirse jerárquicamente para tener las subredes como muestra el esquema de la Fig. 3.4.4.4.3.6.5.

N	16-n		64 bits
SLA1	Subred		Interface ID
	m	16-n-m	64 bits
	SLA2	Subred	Interface ID

Fig. 3.4.4.4.3.6.5 Uso del campo SLA ID para obtener subredes

- **Interface ID:**
  Este es el ultimo campo de la dirección IPv6, es un campo de 64 bits de longitud. Para fines de la autoconfiguración de direcciones y de la movilidad este identificador de interfaz es generado para formar direcciones IPv6 únicas y universales en formato EUI-64 (Extended Universal Identifier de 64 bits) a partir de la dirección física o MAC de la interfase LAN.
  Los prefijos de formato 001 a 111 con excepción de las direcciones multicast requieren tener identificadores de interfase en formato EUI-64.

Agregación de direcciones derivada del formato unicast de agregación global.

Por la forma en que se divide la dirección IPv6 unicast globalmente ruteable (Fig. 3.4.4.4.3.6.1) la agregación basada en este formato se puede realizar, Fig. 3.4.4.4.3.6.6.

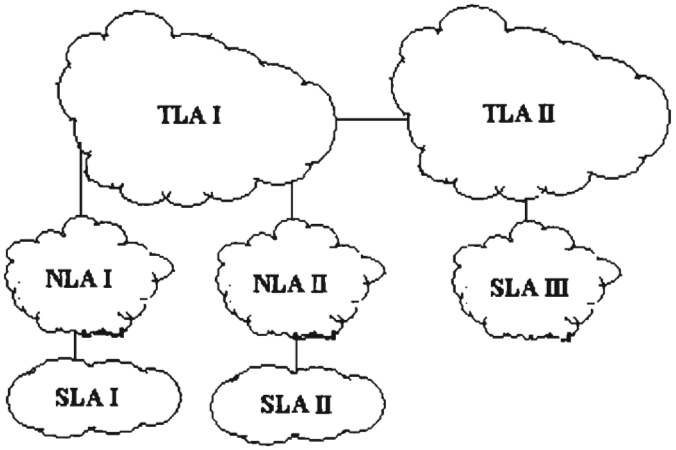


Fig. 3.4.4.4.3.6.6 Esquema de agregación.

Como se observa en la Fig. 3.4.4.4.3.6.6 un TLA tiene varios clientes a los que delega a los cuales proporciona conectividad proporcionándoles un u subconjunto de su espacio de dirección, con lo que aseguran que todo el espacio de dirección que les es anunciado de sus clientes hacia abajo de la jerarquía (downstream) es un subconjunto de su espacio de dirección. Con IPv6 usuarios finales y pequeños proveedores de red NSPs no obtendrán espacios de dirección directamente. Los TLAs se encargaran de administrar y delegar a sus clientes downstream (NLA y SLA) bloques de direcciones.

Reducción de las tablas de ruteo

El esquema de direccionamiento de IPv6 ayuda a minimizar el numero de entradas de ruteo del núcleo de Internet que necesitan ser transportadas, Fig. 3.4.4.4.3.6.7.

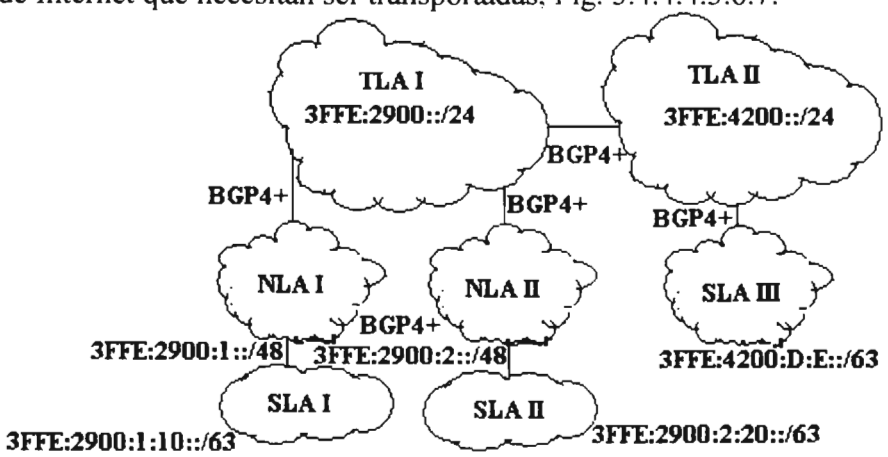


Fig. 3.4.4.4.3.6.7 Ruteo jerárquico IPv6

En la Fig. 3.4.4.4.3.6.7 se puede observar que el TLA I y II intercambian rutas vía BGP, cada uno debe proporcionarle al otro sus rutas.

El TLA 1 delega bloques de direcciones al NLA I y II y estos a su vez delegan parte de sus bloques a SLA I y SLA II
Así el SLA I anuncia su bloque hacia arriba al NLA 1, el cual no anuncia este bloque del SLA I al TLA I. El TLA I solo necesita escuchar las agregaciones que él delega a sus dos NLAs independientemente de cómo ellos las hayan subdelegado. La Fig. 3.4.4.4.3.6.8 nos muestra las rutas anunciadas entre niveles.

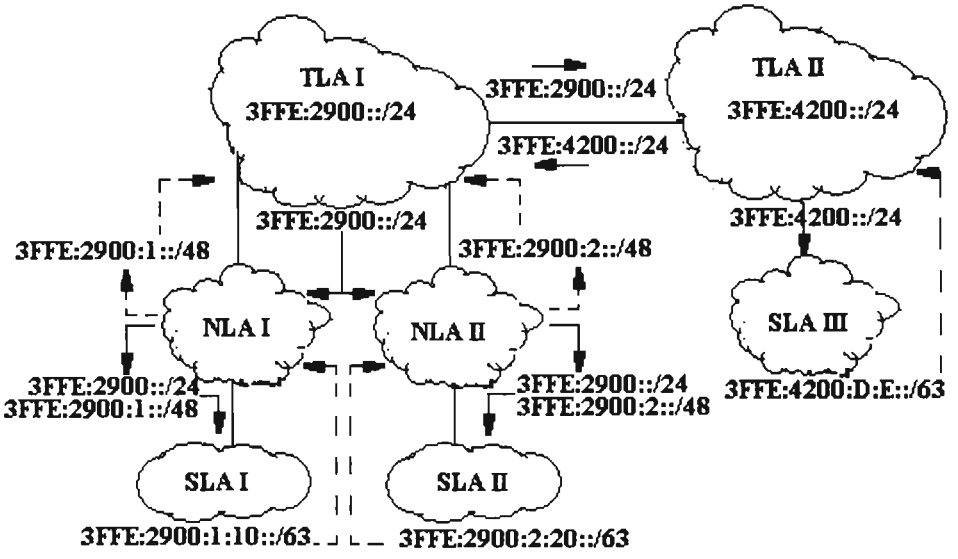


Fig. 3.4.4.4.3.6.8 Anunciamiento de rutas por agregación.

De esta forma el TLA I tiene que transportar tres anunciamientos: 3FFE:2900:1::/48 (NLA I), 3FFE:2900:2::/48 (NLA I), 3FFE:4200::/24 (TLA II).
Pero los dos primeros anunciamientos son subconjuntos de su bloque. Por lo que entre la pareja TLA I y TLA II solamente una ruta necesita ser intercambiada.
Esta es la simplicidad y reducción en el ruteo que proporciona el concepto de agregación de IPv6. Esta simplicidad de ruteo se deriva de que ahora los bloques de direcciones no son portátiles (dirección portátil la que se lleva el usuario consigo cuando cambia de proveedor, lo que conduce a anunciamientos extraños en el núcleo de Internet) y de que ahora solamente a los TLAs se les asignara espacio de las autoridades de numeración.

Formato de la dirección IPv6 unicast de agregación global actual

En los inicios de las implementaciones de IPv6 se definió el formato de la dirección unicast global de agregación en el que el prefijo de ruteo incluía los dos campos jerárquicamente estructurados TLA (Top-Level Aggregator) y NLA (Next-Level Aggregator) pero como estos campos estaban basados en políticas el IETF decidió remover esos campos para tener solamente un prefijo de ruteo global, Fig. 3.4.4.4.3.6.9. Las primeras redes IPv6 pueden aun estar usando esa arquitectura.

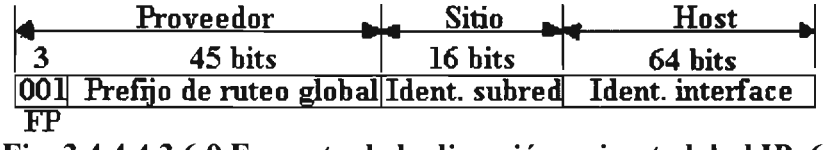


Fig. 3.4.4.4.3.6.9 Formato de la dirección unicast global IPv6

Actualmente las direcciones unicast globales están definidas únicamente por un prefijo de ruteo global que empieza con 001 (2000::/3), un identificador de subred (subnet ID) y un identificador de interfaz (interface ID), con excepción de las direcciones que empiezan con 0000 todas las direcciones unicast globales tienen un identificador de interfase de 64 bits.
De esta forma la dirección IPv6 unicast de agregación global tiene tres partes:

- Prefijo de ruteo global recibido de un proveedor: El prefijo asignado por un proveedor a una organización permitida debería ser de al menos 48 bits (/48). El prefijo de /48 representa los 48 bits de mayor orden de prefijo de red. Ese prefijo asignado a la organización es parte del prefijo del proveedor.
- Identificador de sitio o de subred: Con un prefijo asignado a una organización, es posible que esta habilite hasta 65,535 subredes (asignación de un prefijo de 64 bits a cada subred), ya que la organización puede usar desde 49 a 64 bits del prefijo recibido para subneteo.
- Host: El host usa el identificador de interfaz de cada nodo compuesto de los 64 bits de mas bajo orden.

Así por ejemplo como muestra la Fig. 3.4.4.4.3.6.10.

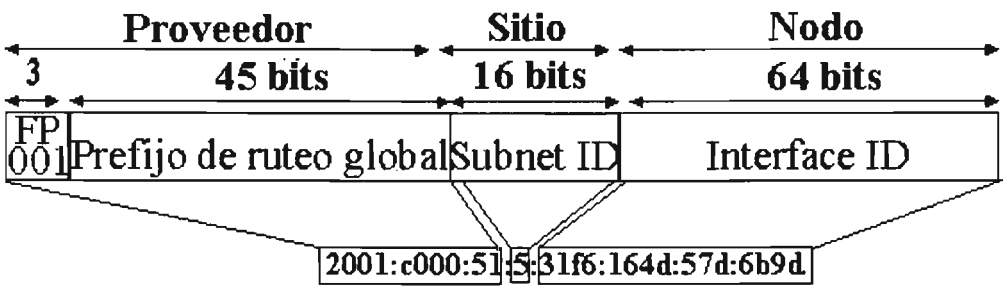


Fig. 3.4.4.4.3.6.10 Ejemplo de asignación de una dirección unicast de agregación global.

El sitio recibe un prefijo de 2001::c000:51:5::/48 asignado por el proveedor. Dentro de la organización el prefijo 2001:c000:51:5::/64 se habilita sobre una subred de la red y finalmente el nodo en esa subred recibe la dirección 2001:c000:51:5:31f6:164d:57d:6b9d /64.

Prefijos TLA asignados

Del prefijo asignado a las direcciones unicast de agregación global, tres prefijos (TLA) más pequeños de 16 bits (/16) se han asignado para uso publico, tabla 3.4.4.4.3.6.1:

- Direcciones unicast de agregación global asignadas por un proveedor que comienzan con 2001::/16 y utilizan un sub-TLA. Este prefijo esta disponible para la producción de Internet.
- Direcciones unicast de agregación global de prueba 6Bone que comienzan con 3FFE::/16. Prefijo asignado para propósitos de prueba del 6Bone.
- Direcciones unicast de agregación global 6to4 que comienzan con 2002::/16. Prefijo reservado para nodos que usan el mecanismo de transición 6to4.

Prefijos	Representación binaria	Descripción
2001::/16	0010 0000 0000 0001	Producción Internet IPv6
2002::/16	0010 0000 0000 0010	Mecanismo de transición 6to4
2003::/16 hasta 3FFD::/16	0010 xxxx xxxx xxxx	Disponible (sin asignar)
3FFE::/16	0011 1111 1111 1110	6Bone

Tabla 3.4.4.4.3.6.1 Prefijos TLA asignados

3.4.4.4.3.7 Direcciones unicast de agregación global asignadas por un proveedor que comienzan con 2001 y utilizan un sub-TLA para servicios de producción.

Se han realizado algunas subdivisones a la estructura de direcciones unicast de agregación global con FP=2000, estas subdivisiones se han hecho para reservar direcciones para aplicaciones, así el campo NLA se ha dividido para agregar un nuevo nivel jerárquico conocido como sub-TLA, Fig. 3.4.4.4.3.7.1.

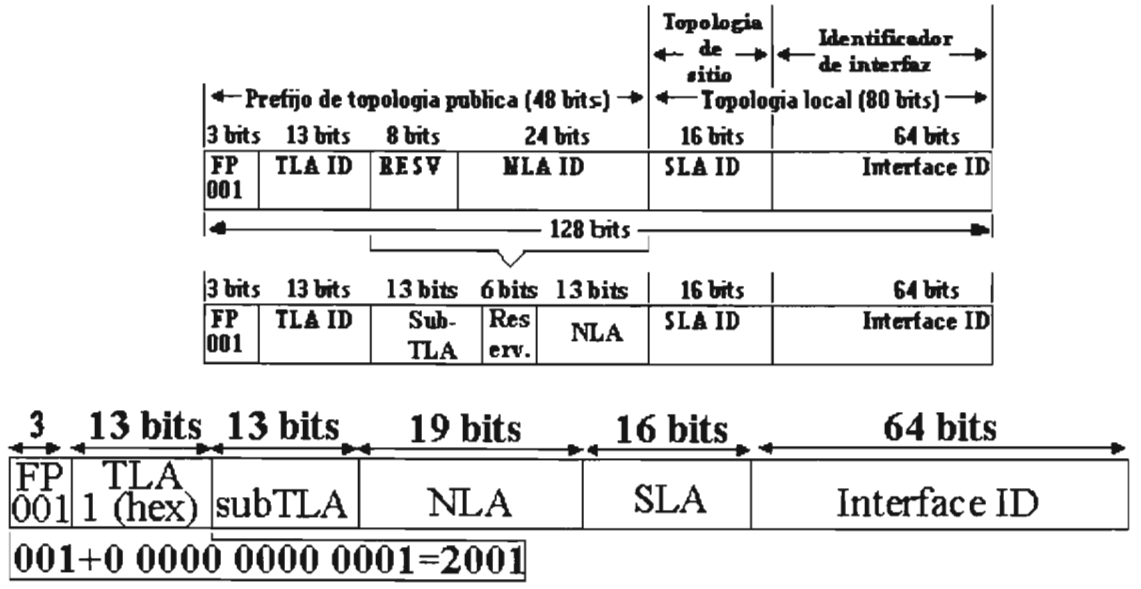


Fig. 3.4.4.4.3.7.1 Direcciones Unicast de Agregación Global (Global Aggregatable Unicast Addresses) con el nuevo nivel jerárquico sub-TLA para producción

De esta manera los campos reservado y NLA se han divido en tres campos, el primero de 13 bits de longitud identifica al sub-TLA, el segundo formado por 6 bits de reserva y el tercero identifica un nuevo campo NLA de solamente 13 bits. El valor dado al campo TLA conocido como TLA1 en este caso es de 0x1, este valor agregado a los tres bits del prefijo FP=001 del plan de agregación global genera un prefijo de 16 bits conocido también como prefijo agregación global de asignación temprana o de lento arranque con valor de 2001::/16 (001+0 0000 0000 0001), así las direcciones de producción comienzan con valor 2001.

Los siguientes 13 bits contienen un subTLA por lo que cada nuevo ISP obtiene un prefijo de 29 bits (/29) o mayor según las necesidades. Cada ISP obtiene menos espacio que un TLA.

En este caso los TLA son llamados sub-TLA, los cuales son asignados mediante un proceso del Registro de Internet Regional Internacional.

3.4.4.4.3.8 Direcciones unicast de agregación global de prueba 6Bone que comienzan con 3FFE.

Se reservo el espacio de un TLA para crear el prefijo 6BONE de 16 bits 3FFE para realizar las pruebas de IPv6 en la red experimental 6BONE, el 6BONE es una red de redes IPv6 mundial que transporta trafico IPv6 sobre túneles IPv4. Estas direcciones son conocidas como direcciones de agregación global de prueba (Aggregatable Global Test Unicast Addresses), en este caso los TLA (Top-level aggregators) son llamados pseudo TLA o pTLA de pruebas y se asignan mediante un proceso definido por la comunidad del 6BONE. Este pTLA agrega los bits 0x1FFE a los 3 bits del prefijo FP=001 del plan de agregación global con lo que se forma el prefijo 3FFE::/16 (001+1 1111 1111 1110), Fig. 3.4.4.4.3.8.1.

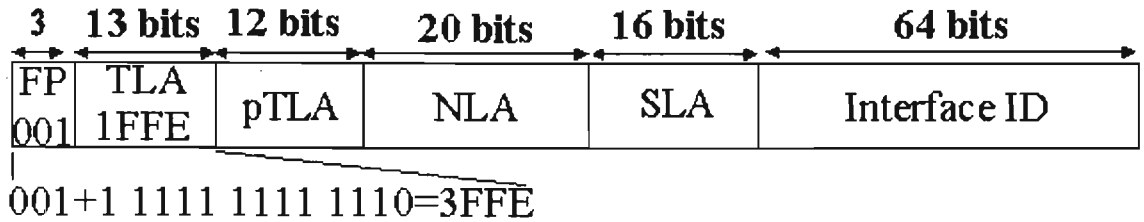


Fig. 3.4.4.4.3.8.1 Direcciones unicast globales para el 6BONE

Los siguientes 12 bits que siguen al prefijo 3FFE asignado al 6BONE contienen el pseudo TLA (pTLA), así los pTLAs son como pISPs de alto nivel y reciben un prefijo de 24 o 28 bits que debe ser administrado con las reglas de los TLA, este prefijo esta dentro del rango 3FFE:0800::/28. Estos pTLAs de pruebas a su vez se encargan de asignar direcciones IPv6 experimentales a sitios secundarios estableciendo una jerarquía de direccionamiento que cumple con el direccionamiento de agregación global., cada pTLA asigna porciones de su espacio a sitios NLA de transito que se conocen como pNLAs (pseudoNLAs) o a sitios terminales sin romper el esquema de agregación. Un sitio final recibe un prefijo /48 de su proveedor upstream y a las LAN dentro del sitio se les asigna un prefijo /64 del prefijo del sitio.

3.4.4.4.3.9 Direcciones unicast de agregación global 6to4 que comienzan con 2002.

Actualmente también se tiene reservado el espacio de un TLA para crear un bloque de direcciones que empiezan con el prefijo 2002, estas direcciones encapsulan las direcciones IPv6 en direcciones IPv4 para poder realizar la conexiones de redes IPv6 hacia la red experimental 6BONE por medio del Internet IPv4, por lo que estas direcciones son conocidas como direcciones de agregación global 6to4 (Aggregatable Global 6to4 Unicast Addresses), el valor dado al campo TLA en este caso es de 0x2, este valor agregado a los tres bits del prefijo FP=001 del plan de agregación global genera un prefijo de 16 bits con valor de 2002::/16 (001+0 0000 0000 0010)conocido como prefijo de agregación global 6to4, fig. 3.4.4.4.3.9.1.

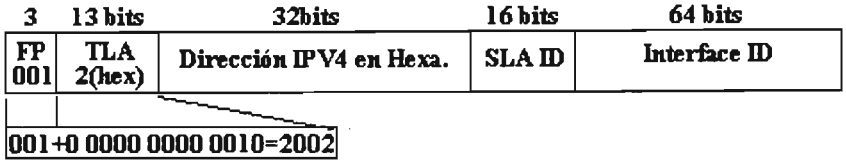


Fig. 3.4.4.4.3.9.1 Formato de las direcciones unicast globales 6to4.

En las direcciones 6to4 los primeros 16 bits son el prefijo 2002::/16, los siguientes 32 bits son formados al tomar la dirección IPv4 publica (globalmente ruteable) del host, la dirección IPv4 se transforma a su equivalente hexadecimal y se inserta en los campos 3 y 4 de la dirección IPv6.

La Fig. 3.4.4.4.3.9.2 resume los formatos de algunos tipos de direcciones IPv6

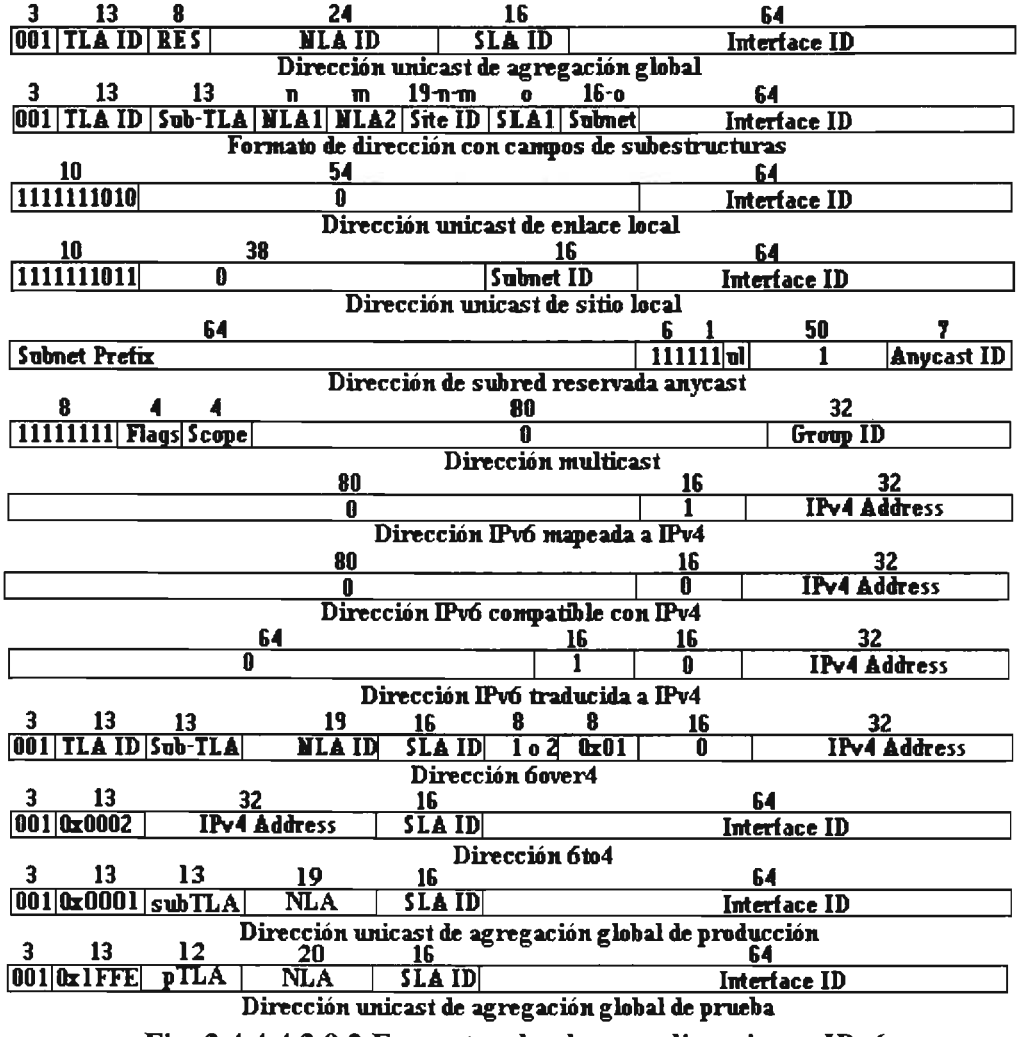


Fig. 3.4.4.4.3.9.2 Formatos de algunas direcciones IPv6

La Fig. 3.4.4.4.3.9.3 resume los tipos de direcciones de la arquitectura de direccionamiento IPv6:

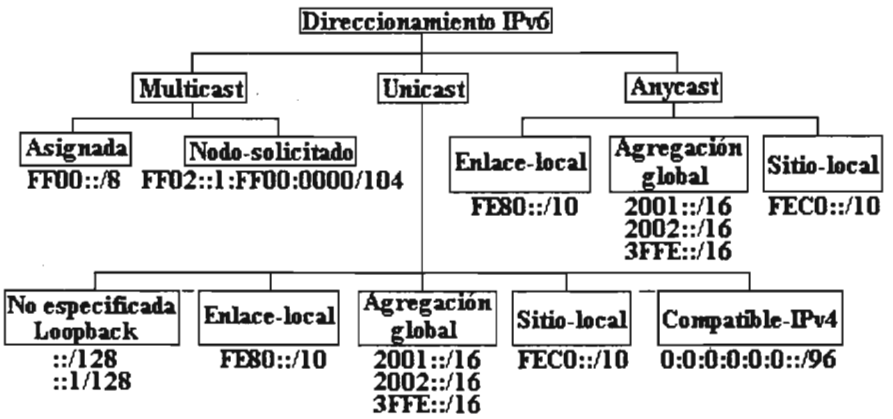


Fig. 3.4.4.4.3.9.3 Tipos de direcciones.

3.4.4.4.4 Espacio de direccionamiento IPv6 reservado y asignado.

La autoridad para números asignados de Internet IANA (Internet Assigned Numbers Authority) es el organismo encargado de administrar el espacio de direccionamiento en base al plan de direcciones de agregación global, la IANA asigna bloques a los organismos regionales para que ellos a su vez realicen asignaciones especificas de direcciones a los ISPs y otros subregistros regionales.
Las organizaciones y personas pueden obtener asignaciones de direcciones directamente de su ISPs
La asignación de direcciones IPv6 se maneja de la misma forma que se realiza en IPv4 mediante los registros regionales basados en la localización geográfica:

- Asia Pacific Network Information Center (APNIC) para Asia y países del pacifico.
- American Registry for Internet Numbers (ARIN) para Norteamerica.
- Reseax IP Europeens-Network Coordination Center (RIPE-NCC) para Europa.

Las direcciones IPv6 solamente son otorgadas a ISPs no a empresas.

Proceso de asignación de direcciones
El tamaño de la asignación de direcciones a un sitio o usuario final es de longitud fija /48.
El proceso completo de asignación de direcciones es en forma general como sigue:

- IANA asigna 2001::/16 a los registros regionales.
- Cada registro obtiene un prefijo de /23 dentro del espacio 2001::16 del IANA.
- Los registros asignan un prefijo de /32 o /35 a un nuevo ISP.
- El ISP asigna un prefijo de /48 a cada cliente.

Esta asignación de prefijos se visualiza en la Fig. 3.4.4.4.4.1.

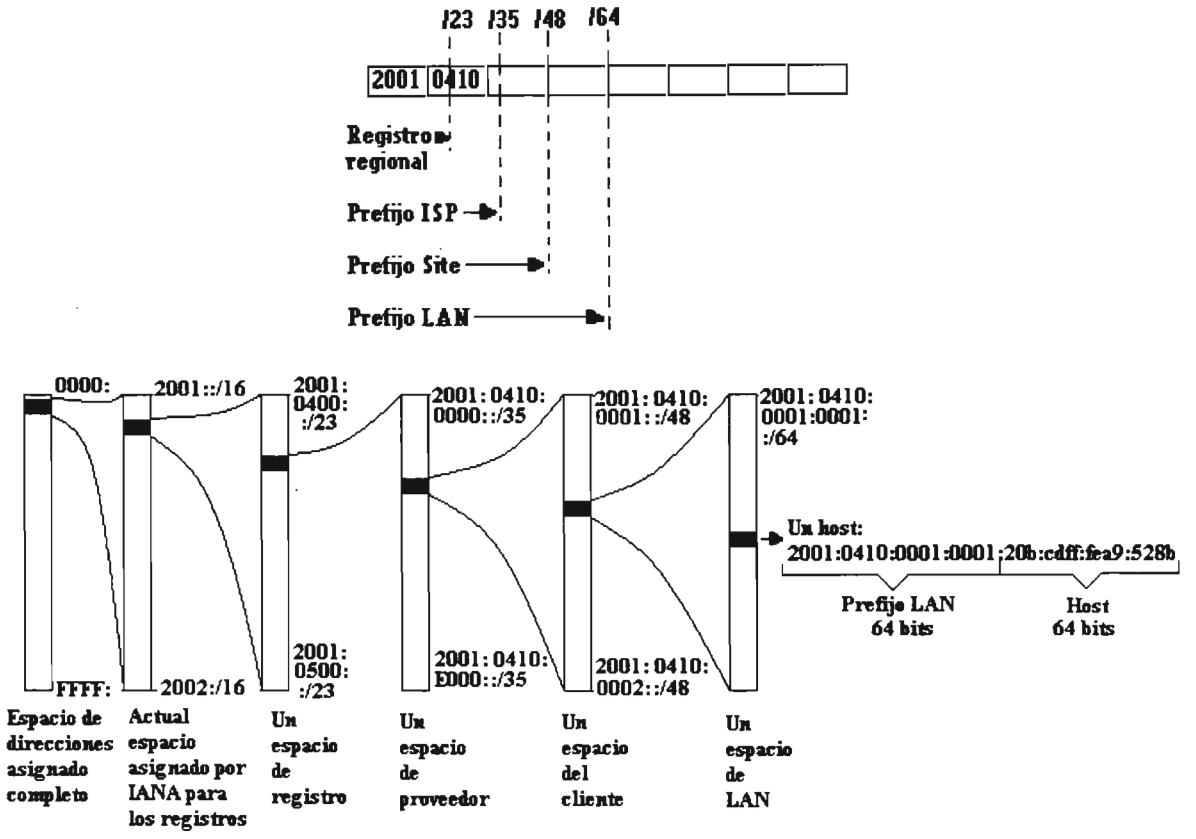


Fig. 3.4.4.4.4.1 Proceso de asignación de direcciones.

La IANA asigna un prefijo /23 dentro del espacio 2001::/16 a los registros regionales, los registros a su vez asignan un prefijo inicial de /32 a los ISPs de IPv6, los ISPs asignan un prefijo /48 a cada cliente o sitio. El prefijo /48 puede ser asignado a cada LAN usando un prefijo /64 para un máximo de identificación de hosts de 64 bits. Cada sitio puede realizar subneteo para un máximo de 65535 LANs.

Para recibir un bloque de dirección con prefijo /32 de un registro, el ISP debe tener un protocolo de ruteo exterior comunicado con al menos otros 3 ISPs y debe tener al menos 40 clientes conectados o demostrar un claro intento de proporcionar servicios IPv6 dentro en un lapso de 12 meses.

La IANA ha empezado a asignar bloques con el prefijo unicast de agregación global 2001::/16 a los organismos regionales como muestra la tabla 3.4.4.4.4.1.

Coordinación regional	Región	Prefijo	Bloque
APNIC	Asia-Pacifico	2001:0200::/23, 2002:0C00::/23, 2002:0E00::/23, 2001:4400::/23, 2001:8000::/19, 2001:A000::/20, 2400:0000::/19	2001:0200::/29-2001:03E8::/29
ARIN	Norteamérica	2001:0400::/23, 2001:1800::/23, 2001:4200::/23, 2001:4800::/23, 2600:0000::/22, 2604:0000::/22, 2608:0000::/22, 260C:0000::/22	2001:0400::/29-2001:05E8::/29
RIPE NCC	Europa	2001:0600::/23, 2001:0800::/23, 2001:1400::/23, 2001:1600::/23, 2001:1A00::/23, 2001:1C00::/22, 2001:2000::/20, 2001:3000::/21, 2001:3800::/22, 2001:4000::/23, 2001:4600::/23, 2001:4A00::/23, 2001:4C00::/23, 2001:5000::/20, 2003:0000::/18, 2A00:0000::/21	2001:0600::/29-2001:07E8::/29
LACNIC	América latina y Caribe	2001:1200::/23	
Documentación		2001:0DB8::/32	Rango no ruteable
Reservado		2001:3C00::/22	Posible asignación futura al RIPE NCC
6to4		2002:0000::/16	Para implementaciones 6to4
6BONE		3FFE:0000::/16	Asignación experimental al 6BONE. Será regresado al pool sin asignar en 2006

Tabla 3.4.4.4.4.1 Asignación de bloques de direcciones con prefijo 2001.

De esta forma la IANA ha empezado a reservar y asignar el espacio IPv6 para ciertos usos como muestra la tabla 3.4.4.4.4.2, donde tenemos el espacio total de direccionamiento y los prefijos reservados.

Tipo o Espacio de asignación	Prefijo del Formato FP (binario). 16 bits de mayor orden	Rango en hexa decimal	Prefijo	Fracción del Espacio de direcciones
(Desaprobada) o reservado	**0000 0000** xxxx xxxx	0000-00FF	0000::/8	1/256
No asignado	**0000 0001** xxxx xxxx	0100-01FF	0100::/8	1/256
Reservado para asignación de OSI/NSAP (Desaprobada)	**0000 001**x xxxx xxxx	0200-03FF	0200::/7	1/128
Reservado para asignación de IPX	**0000 010**x xxxx xxxx	0400-05FF	0400::/7	1/128
No asignado	**0000 011**x xxxx xxxx	0600-0700	0600::/7	1/128
No asignado	**0000 1**xxx xxxx xxxx	0800-0FFF	0800::/5	1/32
No asignado	**0001** xxxx xxxx xxxx	1000-1FFF	1000::/4	1/16
Unicast de Agregación Global (Aggregate Global Unicast)	**001**x xxxx xxxx xxxx	2000-3FFF	2000::/3	1/8
Dirección unicast basada En proveedor-No asignado	**010**x xxxx xxxx xxxx	4000-5FFF	4000::/3	1/8
No asignado	**011**x xxxx xxxx xxxx	6000-7FFF	6000::/3	1/8
Reservado para direcciones Unicast basadas Geográfia-No asignado	**100**x xxxx xxxx xxxx	8000-9FFF	8000::/3	1/8
No asignado	**101**x xxxx xxxx xxxx	A000-BFFF	A000::/3	1/8
No asignado	**110**x xxxx xxxx xxxx	C000-DFFF	C000::/3	1/8
No asignado	**1110** xxxx xxxx xxxx	E000-EFFF	E000::/4	1/16
No asignado	**1111 0**xxx xxxx xxxx	F000-F7FF	F000::/5	1/32
No asignado	**1111 10**xx xxxx xxxx	F800-FBFF	F800::/6	1/64
Unicast local unica	**1111 110**x xxxx xxxx	FC00-FDFF	FC00::/7	1/128
No asignado	**1111 1110 0**xxx xxxx	FE00-FE7F	FE00::/9	1/512
Direcciones unicast locales al enlace (Link-Local Unicast)	**1111 1110 10**xx xxxx	FE80-FEBF	FE80::/10	1/1024
Direcciones unicast locales al sitio (Site-Local Unicast) (Desaprobada)	**1111 1110 11**xx xxxx	FEC0-FEFF	FEC0::/10	1/1024

Direcciones multidistribución (Multicast)	**1111 1111** xxxx xxxx	FF00-FFFF	FF00::/8	1/256
Direcciones unicast de agregación Global para el sub-TLA-producción (IANA)	**0010 0000 0000 0001**	2001	2001::/16	1/63536
Direcciones unicast de agregación Global de prueba	**0011 1111 1111 1110**	3FFE	3FFE::/15	1/32768
Direcciones unicast de agregación Global 6to4	**0010 0000 0000 0010**	2002	2002::/15	1/32768

Tabla 3.4.4.4.2 Asignación de direcciones IPv6 por prefijo del formato (FP)

Las direcciones reservadas (FP=0000 0000 1/256) no se deben confundir con las direcciones sin asignar ya que son usadas por direcciones no especificadas, direcciones de loopback y direcciones IPv6 compatibles con IPv4.

3.4.4.4.5 Direcciones especiales:

Algunas direcciones especiales que se tienen en IPv6 son:

- **Dirección de loopback.**
  Como en IPv4 (127.0.0.1) es una dirección que no sale del mismo equipo, únicamente se usa para probar la pila de TCP/IP del host:

Representación	Valor
Formato preferido	0000:0000:0000:0000:0000:0000:0000:0001
Formato comprimido	0:0:0:0:0:0:0:1=::1
Formato binario	Todos los bits son puestos a 0, excepto el bit 128 es puesto a 1

- **Dirección no especificada**

Es una dirección unicast no asignada a ninguna interfaz. Indica la ausencia de una dirección y es usada para propósitos especiales, por ejemplo cuando un servidor necesita una dirección IPv6 de un servidor DHCPv6 o cuando un paquete es mandado para la detección de dirección duplicada este tipo de dirección es usada.

Representación	Valor
Formato preferido	0000:0000:0000:0000:0000:0000:0000:0000
Formato comprimido	0:0:0:0:0:0:0:0=::
Formato binario	Todos los bits son puestos a 0

- **Direcciones compatibles con IPv4**

Direcciones usadas para crear automáticamente túneles para transportar paquete IPv6 sobre redes IPv4, usando la dirección destino IPv4 dentro de la dirección IPv6 destino.

Representación	Valor
Formato preferido	0000:0000:0000:0000:0000:0000::/96
Formato comprimido	0:0:0:0:0:0::/96=::/96
Formato binario	Los 96 bits de mas alto orden son puestos a 0

0:0:0:0:0:0:w:x:y:z = ::w.x.y.z

- **Dirección mapeada IPv4**

Representación	Valor
Formato preferido	0000:0000:0000:0000:0000:FFFF::/96
Formato comprimido	0:0:0:0:0:FFFF::/96=::FFFF/96
Formato binario	Los 80 bits de mas alto orden son puestos a 0, los siguientes 16 valen FFFF.

0:0:0:0:0:FFFF:w:x:y:z = ::FFFF:w.x.y.z

- **Dirección URL.**

  Las direcciones IPv6 en una dirección URL se deben encerrar entre paréntesis cuadrados ([ ]) en la forma:
  http://[::FFFF:129.144.52.38]:80/index.html
  Esto es para poder distinguir la indicación de conexión a un puerto especifico de los dos puntos usados para separar los campos de una dirección IPv6.

Direcciones IPv6 requeridas por un host.

Como ya se ha mencionado en IPv6 un nodo puede poseer diferentes direcciones IPv6, para su operación apropiada un nodo requiere reconocer las siguientes direcciones:

- Una dirección de enlace local por cada interfaz, FE80::/10. Obtenida inmediatamente cuando el nodo es habilitado con IPv6
- Dirección(es) unicast de agregación global asignadas a las interfaces, 2000::/3. Esta es asignada.
- La dirección de loopback para la interfaz loopback, ::1. Obtenida inmediatamente cuando el nodo es habilitado con IPv6
- Dirección multicast a todos los nodos, FF01::1 y FF02::1. Obtenidas inmediatamente cuando el nodo es habilitado con IPv6
- Dirección multicast de nodo seleccionado para cada una de sus direcciones unicast y anycast asignadas, FF02::1:FFxx:xxxx, donde xx:xxxx son los últimos 24 bits de cada una de sus direcciones unicast y anycast asignadas.
- Direcciones multicast de descubrimiento de vecinos asociadas con todas las direcciones unicast y anycast asignadas a las interfaces.
- Direcciones multicast de todos los otros grupos a los cuales el host pertenece, FF00::/8. Si es miembro de otro grupo multicast.
- Dirección de site local, si es usada, FEC0::/10. Esta es asignada.

Direcciones requeridas por un router.
Por su parte un router además de las direcciones requeridas por un nodo (dirección de enlace local por cada interfaz, direcciones unicast asignadas a interfaces, la dirección de loopback, multicast de descubrimiento de vecinos, multicast de grupos a los que pertenece) requiere las reconocer las siguientes direcciones:

- Todas las direcciones requeridas por un nodo (FE80::/10, 2000::/3, ::1, FF01::1, FF02::1, FF02::1:FFxx:xxxx, FF00::/8, FEC0::/10.
- Direcciones multicast todos-los-nodos, FF01::1, FF02::1.
- Direcciones multicast todos-los-routers, FF01::2, FF02::2, FF05:2
- Direcciones anycast subred-router para todos los enlaces sobre los cuales tiene interfaces configuradas para reenvío, Prefijo Unicast:0:0:0:0.
- Otras direcciones anycast configuradas y asignadas a interfaces.
- Direcciones multicast especificas para protocolos de ruteo.

Direccionamiento a nivel LAN.
Internamente en las redes LAN el direccionamiento IPv6 tiene las siguientes características:
- Las direcciones son asignadas a interfaces.
- Las interfaces pueden tener varias direcciones.
- Las subredes están asociadas con un enlace sencillo.
  - Un enlace es un dominio de la capa de enlace tal como una LAN.
  - No hay cambio desde IPv4.
  - Múltiples subredes sobre un enlace.

Las direcciones de los nodos pueden tener múltiples direcciones como pueden ser:

- Direcciones de link-local.
  - Validas sobre enlaces específicos como LANs.
  - Para comunicación entre nodos del mismo enlace.
- Direcciones de site-local.
  - Validas solo dentro de una organización particular.
- Direcciones de alcance global (global scope).
  - Globalmente única.
  - Puede ser usada en cualquier parte.

3.4.5 Protocolos, servicios y aplicaciones

Como ya se ha mencionado la nueva versión de IP es totalmente compatible con IPv4 por lo que proporciona los mismos servicios que IPv4 y tiene las mismas aplicaciones, además de los nuevos que se están desarrollando. En el caso de los protocolos sucede algo similar, los protocolos que componen a IPv6 son producto de la actualización de los protocolos existentes en IPv4 e implementan las nuevas funcionalidades de IPv6.

Protocolos de IPv6
Algunos de los nuevos protocolos de IPv6 se resumen a continuación:

- ICMPv6
- DHCP6
- Neighbor discovery

- DNS
- MLD
- Protocolos de ruteo

3.4.5.1 ICMPv6

El protocolo de mensajes de control (Internet Control Message Protocol) ICMPv4 es parte integral de IPv6 con algunos cambios (ICMPv6) y se debe implementar completamente en cada nodo IPv6. Este protocolo combina funciones que antes estaban divididas entre diferentes protocolos como ICMP, IGMP y ARP.
ICMPv6 es de uso obligatorio en IPv6 ya que es usado por los nodos IPv6 para reportar errores encontrados en el procesamiento de paquetes, diagnósticos de desempeño y para ejecutar otras funciones de capa de Internet como diagnósticos mediante la utilería ping. Maneja dos clases de mensajes:

- Mensajes de error. Estos mensajes tienen un valor cero en el bit de mayor orden de su campo tipo por lo que pueden tomar un valor entre el rango 0 a 127.
- Mensajes informativos. Estos mensajes tienen en su mensaje un valor de entre 128 y 255 para el campo tipo.

La estructura de los mensajes ICMPv6 se muestra en la Fig. 3.4.5.1.1.

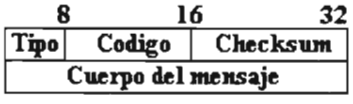


Fig. 3.4.5.1.1 Campos de un mensaje ICMPv6

Donde los campos son los siguientes:

- Tipo: Este campo de 8 bits indica el tipo de mensaje. Si el bit de mayor orden vale cero (valores en el rango 0-127) es un mensaje de error, si vale 1 (valores en el rango 128-255) es un mensaje informativo.
- Código: Aplica una clasificación adicional al tipo de mensaje.
- Checksum: Detecta errores.

La tabla 3.4.5.1.1 muestra algunos mensajes de error e informativos de ICMPv6.

Mensajes de error		
Tipo	Descripción y códigos	
1	Destino inalcanzable (destination unreachable)	
	Código	Descripción
	0	Sin ruta al destino
	1	Prohibido administrativamente
	2	Sin asignar
	3	Dirección inalcanzable
	4	Puerto inalcanzable
2	Paquete demasiado grande	
3	Tiempo excedido (Time exceded)	
	Código	Descripción
	0	Limite de saltos excedido
	1	Tiempo de defragmentación excedido
4	Problema de parámetros	
	Código	Descripción
	0	Encabezado erróneo
	1	Siguiente encabezado desconocido
	2	Opción IPv6 desconocida
Mensajes informativos		
Tipo	Descripción	
128	Solicitud de echo	
129	Respuesta de echo	
133	Router solicitation	
134	Router advertisement	
135	Neighbor solicitation	
136	Neighbor advertisement	
137	Redirect	

Tabla 3.4.5.1.1 Mensajes informativos y de error de ICMPv6

Mensajes de error

La estructura de los mensajes de error se muestra en la Fig. 3.4.5.1.2

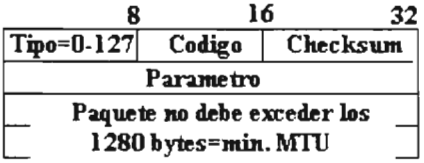


Fig. 3.4.5.1.2 Formato de los mensajes de error

- El mensaje Destination Unreachable es generado cuando la red debe descartar un paquete IPv6 debido a que el destino es inalcanzable. El paquete no debe exceder los 576 bytes. Este tipo de mensaje es generado por un router o un nodo destino que

no puede entregar el mensaje, por lo que se ven forzados a descartar el mensaje. El paquete será desechado sin generar un mensaje si la red esta congestionada. Las razones que provocan este mensaje son:

- o No existe ruta al destino, ya que el router no tiene una entrada en su tabla hacia la dirección destino y no sabe por que interfase retransmitir el mensaje.
- o Comunicación administrativamente prohibida debido a la existencia de equipos de seguridad.
- o No existe el vecindario entre la dirección destino y algún router de los enlaces.
- o Puerto inalcanzable, debido a que el paquete llego al destino pero el protocolo de capa superior es inalcanzable.
- El mensaje Packet Too Big se genera cuando la red descarta un paquete IPv6 debido a que su tamaño excede el MTU del enlace de salida. Esta información es parte de procedimiento de descubrimiento del path MTU.
- El mensaje Time Exceded se genera cuando un router descarta un paquete IPv6 debido a que su campo Hop Limit es cero o se decrementa a cero. El mensaje indica la posible existencia de ya sea un lazo de ruteo o un valor Hop Limit inicial muy pequeño. Otra razon es la imposibilidad de reensamblar un paquete fragmentado dentro del limite de tiempo permitido.
- El mensaje Parameter Problem se genera cuando un nodo IPv6 debe descartar un paquete por que detecta problemas en un campo del encabezado IPv6 o de un encabezado de extensión. Puede detectar los siguientes tres errores:
- o Campo de encabezado erróneo: Un valor ilegal en algún campo del encabezado se ha detectado.
- o Siguiente encabezado no reconocido: La implementación IPv6 no reconoce el siguiente encabezado.
- o Opción IPv6 no reconocida: El paquete contiene una opción no reconocida por la implementación IPv6.

Un mensaje de error nunca debe ser mandado en respuesta a otro mensaje de error.

Mensajes informativos

Los mensajes informativos se subdividen en tres grupos: mensajes de diagnostico, mensajes para administración de grupos multicast y mensajes de descubrimiento de vecinos. La estructura de los mensajes informativos se muestra en la Fig. 3.4.5.1.3

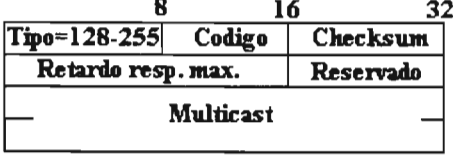


Fig. 3.4.5.1.3 Formato de los mensajes informativos.

- El mensaje Echo Request y su correspondiente Echo Reply son mensajes de diagnostico y son usados para implementar la aplicación de diagnostico ping que nos permite checar si un destino es alcanzable.
- El mensaje Echo Reply debe ser implementado por cada nodo IPv6 para que reciba echo requests y mande los correspondientes echo replies

- Los mensajes de Group Membership Messages transportan información acerca del numero de miembros de grupo multicast de los nodos sus routers vecinos, sus tipos de mensajes son:
  - Mensaje Group Membership Query donde la dirección destino es igual a la dirección multicast del grupo solicitado o a la dirección de todos los nodos del enlace local FF02::1
  - Mensaje Group Membership Report o Group Membership Reduction, donde la dirección destino es igual a la dirección multicast del grupo reportado o terminado.
- Los mensajes Router Solicitation son usados por los nodos IPv6 para pedir a los routers que generen mensajes anunciamientos de router inmediatamente. La dirección fuente de estos mensajes es la dirección unicast de la interfase que manda el mensaje o si no tiene, se usara la dirección no especificada. La dirección destino es el grupo multicast de todos los routers FF02::2. El campo Hop Limit del encabezado IPv6 se pone a 255 para evitar el ataque de hackers, los routers verifican que el campo tenga este valor, si no descartan el paquete. Un hacker nunca podrá enviar un mensaje con Hop Limit igual a 255 desde el exterior de la LAN ya que este se decrementaria por lo menos en 1. Solo los paquetes generados en la LAN pueden tener este campo igual a 255.
- Los mensajes Router Advertisement son enviados periódicamente o en respuesta a mensajes de solicitud de router. La dirección fuente es la dirección de enlace local de la interfase que manda el mensaje y la dirección destino es igual a la del nodo que solicito el mensaje o la dirección multicast de todos los nodos FF02::1. EL campo de 1 bit M (configuración de dirección administrada) indica que el nodo que reciba el anunciamiento debe usar el protocolo stateful para la autoconfiguración de dirección además de la autoconfiguración stateless. El campo de 1 bits O (otra configuración stateful) indica que el nodo que reciba el anunciamiento debe usar el protocolo de autoconfiguración stateful para información adicional. El campo Router Lifetime contiene el tiempo en segundos durante el cual el router puede ser usado como default router, si es cero el router no puede ser usado como default router. Este mensaje tiene las siguientes opciones:
  - Opción que especifica la dirección de capa de enlace del nodo fuente.
  - Opción que especifica el MTU del enlace.
  - Opción de información de prefijo que indica el prefijo a ser usado para la autoconfiguración de dirección. Un router debería incluir todos sus prefijos para que los hosts multihomed se autoconfiguren correctamente.
- Los mensajes Neighbor Solicitation solicitan direcciones de capa de enlace de nodos destinatarios mientras proporcionan la dirección de capa de enlace de la fuente. Son mandados a direcciones multicast cuando un nodo necesita resolver una dirección o a direcciones unicast cuando se quiere checar la alcanzabilidad de un vecino. La dirección fuente puede ser la dirección unicast de la interfase que transmite el mensaje o durante el procedimiento de detección de dirección duplicada la dirección no especificada.
- Los mensajes Neighbor Advertisement son enviados cuando el estado de un nodo cambia para propagar las modificaciones rápidamente y en respuesta a mensajes de solicitud de vecino. La dirección fuente es la dirección de la interfase que manda el mensaje y la dirección destino puede ser la del nodo que solicito el mensaje o la dirección multicast de todos los nodos FF02::1. El campo de 1 bit R indica que el

nodo fuente es un router. El campo S indica que el mensaje e suna respuesta a una solicitud de vecino. El campo O indica que el mensaje debería actualizar la dirección de capa de enlace almacenada.

- Los mensajes Redirect son enviados por los routers para informar a otros nodos de un mejor primer salto hacia el destino. Con estos mensajes los hosts pueden ser direccionados a otro router conectado al mismo enlace o a otro vecino. La dirección fuente es igual a la dirección de enlace local de la interfase que manda el mensaje y la dirección destino es la dirección fuente del paquete que causo el mensaje Redirect. La dirección Target contiene la dirección del nodo que solicito el mensaje, si esta es el punto final de la comunicación debe contener el mismo valor de la dirección destino, o de otra forma tendrá el valor de la dirección de enlace local de un router que el mejor primer salto hacia el destino. La dirección Destination es la dirección IPv6 del destino que es redireccionado a la dirección Target.
- Opciones:
  - Opción de dirección tipo 1 igual a la dirección de capa de enlace fuente es la dirección del transmisor del paquete, usada en mensajes de solicitud de router, anunciamiento de router y solicitud de vecinos y tipo 2 igual a la dirección de capa de enlace destino usada en mensajes de anunciamiento de vecinos y redireccionamiento. La dirección de capa de enlace es de longitud variable, la mínima longitud es de 48 bits para el transporte de direcciones MAC sobre las LAN.
  - La opción de información del prefijo proporciona a los hosts los prefijos para la autoconfiguración de direcciones. El campo L indica si el prefijo puede ser usado para la determinación de direcciones dentro del enlace (on-link), cuando este campo no es encendido algunas direcciones pueden estar dentro del enlace y otras fuera (off-link). El bit A indica si el prefijo puede ser usado para la autoconfiguración de dirección autónoma. El campo valid lifetime indica los segundos que la dirección autoconfigurada por el prefijo vía stateless es valida, un valor FFFFFFFF significa infinito. El campo preferred lifetime indica los segundos que la dirección autoconfigurada por el prefijo vía stateless es preferida, un valor FFFFFFFF significa infinito.
  - La opción MTU es usada en mensajes de anunciamiento de router para asegurarse que en los enlaces con MTUs variables todos los nodos usen el mismo MTU.

Los mensajes ICMPv6 son transportados dentro de un paquete IPv6 y son identificados por el campo next header con el valor 58.

En IPv6 los paquetes de ICMPv6 pueden ser encriptados con IPsec para la protección de los sistemas contra ataques realizados con ICMP.

3.4.5.2 Protocolo DHCPv6

El protocolo DHCP para IPv6 (DHCPv6) es un protocolo cliente/servidor que trabaja con el protocolo de transporte UDP, DHCPv6 se diseño para facilitar la administración de nodos IPv6 en ambientes donde se debe tener mas control sobre la asignación de direcciones IPv6 y configuración de parámetros, este es un control mejor que el proporcionado por la autoconfiguración sin servidores (stateless). El uso de DHCPv6 reduce el costo de centralizar la administración de recursos de red.

El protocolo DCHP6 basa su funcionamiento en 2 características de IPv6, la primera es la autoconfiguración que realizan los equipos de una dirección de enlace local al momento de conectarse a la red (DHCPv6 es compatible con la autoconfiguración stateless) y la segunda es la posibilidad de multicast de IPv6.
DHCPv6 introduce el concepto de relay, el cual es un nodo que opera como intermediario en la transmisión de un paquete entre un servidor y un cliente. Además del concepto de agente que puede funcionar como servidor o como relay.
Inicialmente el cliente debe detectar la presencia de routers en el enlace mediante mensajes de descubrimiento de vecinos (ND). Si se encuentra algún router, el cliente examina los datos de anunciamiento de router para determinar si DHCP debería ser usado. Si los anunciamientos de router permiten el uso de DHCP o si no es encontrado un router, el cliente pasa a la fase de solicitud de DHCP para encontrar un servidor DHCP.
DHCPv6 esta diseñado para ser extensible para transportar nuevos parámetros de configuración agregando nuevas opciones DHCP que transportan esta información.
Los tipos de mensajes usados por DHCPv6 son:

- Mensaje de solicitud DHCP. Este mensaje es usado cuando el cliente no conoce ningún servidor o quiere localizar un nuevo servidor. Este tipo de mensaje es enviado por el cliente a la dirección multicast de todos los agentes DHCP Servidor/relay (FF02::C).
- Mensaje de anuncio DHCP. Este mensaje unicast es enviado por un agente a un cliente en respuesta a un mensaje de solicitud DHCP.
- Petición DHCP. Mensaje unicast de un cliente a un servidor para pedir parámetros para configuración de la red.
- Respuesta DHCP. Mensaje unicast de un servidor a un cliente en respuesta a una petición DHCP, indica los recursos (direcciones y parámetros) que el servidor asigno al cliente.
- Liberación DHCP. Mensaje unicast mandado del cliente al servidor para informar que el cliente libero ciertos recursos que pueden ser reasignados a otros clientes.
- Reconfiguración DHCP. Mensaje unicast mandado por el servidor para informar al cliente de modificaciones en la red.

De esta forma un equipo que requiere una dirección una vez que autoconfiguró la dirección de enlace local, usando esta dirección como fuente mandara un mensaje de búsqueda del servidor DHCP por medio de multicast a todos los servidores DHCP FF02::1:3 y a todos los agentes de intercambio FF02::1:2. Este mensaje es mandado por medio del protocolo UDP al puerto 547 UDP de servidores y enrutadores y el cliente espera la respuesta en el puerto 546 de UDP, el formato del mensaje de búsqueda DHCP es mostrado en la Fig. 3.4.5.2.1.

Tipo de mensaje	C	A	Reservado
Dirección de enlace local del cliente (16 bytes)			
Dirección de agente de intercambio (16 bytes, si esta presente)			

Fig.3.4.5.2.1 Mensaje de búsqueda DHCP

Mensaje de búsqueda DHCP. Si un agente de intercambio DHCP recibe el mensaje, llenara la dirección relay address con la dirección global o de sitio local de su interfaz receptora,

pondrá el bit A en 1 y entregara el mensaje a todos los servidores DHCP FF05::1:3, los servidores contestan con un mensaje que tiene el formato de la Fig. 3.4.5.2.2.

Tipo de mensaje	S	Reservado
Dirección de agente de intercambio (16 bytes)		
Dirección de enlace local del cliente (16 bytes)		
Direcciones del servidor (16 bytes, si esta presente)		
Extensiones (numero variable y longitud)		

Fig. 3.4.5.2.2 Mensaje de anuncio DHCP

Si el mensaje de búsqueda se recibió directamente en la dirección del agente se pondrá la dirección del servidor, en caso contrario será la dirección del agente y la dirección del servidor se agrega después de la del cliente. El numero variable de extensiones son los parámetros de configuración que pueden ser usados directamente por los clientes. El cliente recibe varios mensajes de anuncio, si no recibe respuesta repetirá la solicitud hasta recibir contestación. Por su parte los agentes envían los anuncios en broadcast para informar que el servicio de configuración esta disponible. Cando el cliente recibe el anuncio seleccionara un agente y un servidor solicitando los parámetros de configuración con mensaje de solicitud que tienen el formato de la Fig. 3.4.5.2.3.

Tipo de mensaje	S	C	Reservado	Identifica. de Transacción
Direcciones del servidor (16 bytes, si esta presente)				
Dirección de agente de intercambio (16 bytes)				
Dirección de enlace local del cliente (16 bytes)				
Extensiones (numero variable y longitud)				

Fig. 3.4.5.2.3 Mensaje de solicitud DHCP

Estos mensajes son enviados directamente a un servidor o vía un agente, el identificador de transacción es un numero proveniente de la secuencia de solicitudes de la maquina que relaciona solicitudes y respuestas. Las solicitudes son entregadas por el agente y recibidas por un servidor, este regresa un mensaje de respuesta al agente, ese mensaje será entregado por el agente a la dirección de enlace local del cliente. Si la solicitud tuvo éxito el código de error es cero, de lo contrario se indica la causa de la falla. Este mensaje tiene el formato de la Fig. 3.4.5.2.4.

Tipo de mensaje	I	Codigo de error	Identifica. de Transacción
Dirección de enlace local del cliente (16 bytes, si esta presente)			
Extensiones (numero variable y longitud)			

Fig. 3.4.5.2.4 Mensaje de respuesta DHCP

Si las solicitudes se envían mediante un agente de intercambio el mensaje contiene la dirección de servidor donde las solicitudes deben ser repetidas, cuando las respuestas tienen que ser entregadas por un agente de intercambio se debe poner la dirección de enlace local del cliente.
Los campos de extensión de las solicitudes y respuestas contienen una lista de parámetros o extensiones que los servidores deben proveer. Los parámetros tienen un formato de longitud variable, el formato de los campos de extensión se muestra en la Fig. 3.4.5.2.5.

Ext-	Ext-	C	L	D	Q	A	P	Reservado	Tamaño del Prefijo
Dirección del cliente (Si esta presente 16 bytes)									
Tiempo de vida preferido (si esta presente 4 bytes)									
Tiempo de vida valido (si esta presente 4 bytes)									
Nombre del DNS (Si esta presente, longitud variable)									

Fig. 3.4.5.2.5 Campos de extensión DHCP

La extensión de dirección es una de las más importantes, la cual incluye cuatro campos indicados por banderas, si el bit C=1 la dirección del cliente esta presente y es una dirección IPv6 registrada en el equipo, si L=1 la extensión contiene los tiempos de vida recomendado y valido de la dirección especificada. Los bits Q, A y P especifican el trato que el cliente requiere para su dirección, si Q=1 solicitara al servidor que el valor de sus parámetros sea definitivo, de lo contrario el servidor podrá reemplazarlos con otros valores. El bit A indica que el servidor registre la dirección en un registro AAAA del servidor DNS, a su vez el bit P indica que el servidor apunte un registro PTR en el DNS que asocie el nombre a la dirección IPv6.
El servidor que asigna la dirección pone el bit D=1 si el cliente no necesita checar si la dirección esta duplicada, el bit A=P=1 si los registros AAAA y PTR están insertados en el DNS, indicara la longitud en bits del prefijo en el campo de tamaño de prefijo. Con los tiempos de vida indicados los equipos son avisados que la dirección no es de su propiedad, solo temporal, para asegurar la propiedad continua se deben repetir las solicitudes DHCP antes que el tiempo de vida termine o de lo contrario el servidor asume que los equipos no requieren mas la dirección y proceden a asignar la dirección a otros clientes.
Además de la extensión de direcciones se tienen otras en DHCP como la extensión del servidor DNS que provee una lista de direcciones IPv6 de los servidores DNS, la extensión del nombre de dominio informa a los clientes del nombre de dominio local, etc.
Los beneficios de usar DHCPv6 son:

- Permite tener mayor control que la autoconfiguración serverless/stateless.
- Se puede usar en ambientes donde no existen routers solamente servidores.
- Se puede usar conjuntamente con la autoconfiguración stateless.
- Los clientes DHCP no requieren configuración manual de parámetros de red.
- Se puede usar para ayudar en la renumeración de redes.
- Se puede usar para el registro de nombres de dominio automático usando DNS dinámico.
- Se puede usar para delegar prefijos IPv6 a routers propiedad del cliente permitidos.

- No se requiere un servidor en cada enlace.
- DHCP contiene los mecanismos apropiados de time out y retransmisión para trabajar eficientemente en ambientes con características de alta latencia y ancho de banda pequeño.

Las características de DHCPv6 son:

- Se pueden configurar las actualizaciones dinámicas al DNS.
- Desaprobación de dirección para la renumeración dinámica.
- Puede usar la autenticación.
- Los clientes pueden solicitar varias direcciones IP.
- Permite la integración de los mecanismos de autoconfiguración de dirección stateless y stateful.

3.4.5.3 Protocolo Neighbor Discovery

El protocolo para el descubrimiento de vecinos ND (neighbor Discovery) permite administrar la interacción entre diferentes nodos conectados al mismo enlace, se usa para implementar la característica de autoconfiguración de direcciones, para conocer la dirección física de los nodos destino por lo que este protocolo es el sustituto del protocolo ARP usado en IPv4, para el descubrimiento de ruteadores y vecinos en el mismo enlace local, con los cuales se tiene conectividad.

Los nodos (hosts y routers) usan ND para determinar las direcciones físicas de vecinos ya conocidos que se encuentran conectados en el mismo enlace, de esta forma estos nodos actualizan en su tabla de almacenamiento valores que se han vuelto inválidos.

Los hosts usan ND para descubrir routers vecinos dispuestos para el envío de paquetes en su nombre.

Los nodos usan ND para mantener un registro de cuales vecinos son alcanzables y cuales no, al mismo tiempo que se detectan cambios de direcciones físicas.

ND define los mecanismos para resolver temas de interacción entre nodos como: descubrimiento de routers vecinos, descubrimiento y aprendizaje de prefijos, descubrimiento de parámetros de direcciones, autoconfiguración de dirección, establecimiento de relaciones entre direcciones de capa de enlace y direcciones IPv6 para la resolución de dirección, determinación del siguiente salto, detección de vecino inalcanzable NUD (Neighbor Unreachable Detection), detección de dirección duplicada DAD (Duplicate Address Detection), redirección del primer salto.

Para llevar a cabo estas funciones el protocolo ND agrega algunos nuevos tipos de mensajes, Fig. 3.4.5.3.1 a ICMPv6 como son:

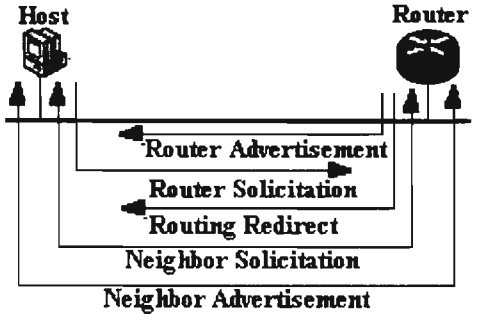


Fig. 3.4.5.3.1 Tipos de mensajes Neighbor Discovery y su dirección.

- Router Solicitation:
  Con este tipo de mensaje identificado con el tipo 133, las interfaces piden a los routers que se anuncien al momento de su conexión al enlace. Al iniciar los hosts mandan mensajes (a la dirección multicast de todos los router conectados al enlace) de solicitud de router para solicitar a los routers que generen anunciamientos de router inmediatamente, sin esperar la transmisión periódica de Router Advertisement, Fig. 3.4.5.3.2.

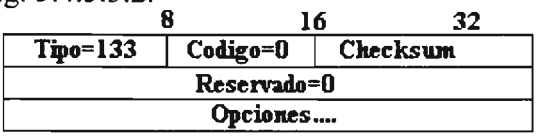


Fig. 3.4.5.3.2 Formato del mensaje de solicitud de router

- Router Advertisement:
  Estos mensajes permiten a los hosts conocer cuales routers están presentes sobre un enlace automáticamente En los enlaces que tienen capacidad de hacer multicast los routers periódicamente envían mediante multicast un paquete de anunciamiento de router. Estos mensajes también son enviados en forma de multicast por los ruteadores como respuesta a la petición de solicitud de router hecha por la interfaz de algún nodo. Dichos mensajes son recibidos por todos los hosts conectados a un enlace, los cuales almacenan en su memoria local la presencia de los routers (Default Router List). Este mensaje tipo 134 es usado por los ruteadores para anunciar su presencia, además de enviar ciertos parámetros necesarios para la autoconfiguración de direcciones como una lista de prefijos de red (usados para determinación del enlace y configuración de dirección), tiempo de vida, etc., la Fig. 3.4.5.3.3 muestra el formato del mensaje de anunciamiento de router:

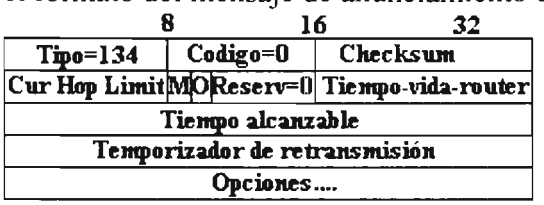


Fig. 3.4.5.3.3 Formato del mensaje de anunciamiento de router.

Los campos del formato del mensaje de anunciamiento de router son los siguientes:

- Tipo: Este campo de 8 bits indica el tipo de mensaje=134
- Código: Aplica una clasificación adicional al tipo de mensaje, su valor es 0
- Checksum: Detecta errores.
- Current Hop Limit: Este debería ser el valor que se ponga en el campo Hop Count del encabezado IP para los paquetes de salida.
- M: Bandera de 1 bit que indica si la configuración de dirección es administrada.
- O: Bandera de 1 bit que indica algún otro tipo de configuración del tipo stateful (por ej. Basada en servidor).
- Router life time: Es un entero de 16 bits que indica el tiempo de vida del router.
- Reachable time: Entero de 32 bits que indica el tiempo alcanzable.
- Retrans timer: Entero de 32 bits que indica el tiempo de retransmisión.

- Opciones: Parámetros opcionales como la dirección de capa de enlace fuente, MTU, etc.
  Los hosts reciben anunciamiento de todos los routers con lo que construyen una lista de los routers por default. Con estos mensajes el router le indica al host como debe ejecutar la autoconfiguración de dirección.

➢ Neighbor Solicitation:
Estos mensajes permiten a todos los nodos (hosts y routers) hacer mapeos entre direcciones IPv6 y direcciones de enlace a través de mensajes Neighbor Solicitation. Este mensaje identificado como tipo 135 es usado por los nodos para solicitar la dirección física del nodo con el que se desea entablar comunicación o para checar si otro nodo aun es alcanzable a través de la dirección almacenada en la memoria, al mismo tiempo que proporcionan su propia dirección física al nodo destino. Este mensaje también es usado en la fase de autoconfiguración para detectar la presencia de direcciones duplicadas. La solicitud de vecino se realiza mediante mensajes multicast cuando el nodo necesita resolver una dirección y se realiza mediante mensajes unicast cuando se quiere verificar la alcanzabilidad de un vecino, el formato de estos mensajes se muestra en la Fig. 3.4.5.3.4:

8	16	32
Tipo=135	Codigo=0	Checksum
Reservado=0		
Dirección destino		
Opciones....		

Fig. 3.4.5.3.4 Formato del mensaje de solicitud de vecino.

Donde:

- Dirección destino: Es la dirección IP del destino de la solicitud que no debe ser una dirección multicast.
- Opciones: Una posible opción puede ser la dirección física origen.

➢ Neighbor Advertisement:
Estos mensajes permiten a todos los nodos (hosts y routers) hacer mapeos entre direcciones IPv6 y direcciones de enlace a través de mensajes Neighbor Advertisement. Un nodo manda mensajes de anunciamiento de vecino ya sea para responder a los mensajes de solicitud de vecino, periódicamente o para propagar nueva información rápidamente. Cuando un nodo recibe este tipo de mensaje actualiza su Neighbor Cache que contiene el mapeo entre direcciones IPv6 y direcciones de capa 2. Estos mensajes junto con los de solicitud de vecinos reemplazan al protocolo ARP de IPv4. La respuesta a una solicitud de vecino se realiza con el mensaje tipo 136, Fig. 3.4.5.3.5.

8	16	32
Tipo=136	Codigo=0	Checksum
R S O	Reservado=0	
Dirección destino		
Opciones....		

Fig. 3.4.5.3.5 Formato del mensaje de anunciamiento de vecino.

Donde:

- Dirección destino: El valor de este campo depende de que si este mensaje fue solicitado o no. Si este mensaje es una respuesta al mensaje de solicitud de vecino, el valor de este

campo es el del campo Target Address en el mensaje de solicitud de vecino que solicito este anunciamiento. Si el anunciamiento no fue solicitado, el valor de este campo es la dirección de quien la dirección física ha cambiado. El valor del campo Target Address no debe ser una dirección multicast.

Resolución de direcciones

Los nodos IPv6 ejecutan la resolución de direcciones IPv6 en direcciones de capa de enlace a través de los mensajes Neighbor Solicitation (NS) y Neighbor Advertisement (NA). Un nodo activa la resolución mandando un mensaje NS multicast de nodo solicitado (que incluye la dirección de capa de enlace de la fuente), solicitando al nodo destino que regrese su dirección de capa de enlace en un mensaje NA. Una pareja de mensajes es suficiente para implementar la resolución.

Detección de dirección duplicada

El mensaje NS se utiliza para determinar si la misma dirección unicast se ha asignado a mas de un nodo.

Detección de inalcanzabilidad de vecino

Los mensajes NS también se usan para detectar sin un nodo es alcanzable mediante el regreso de confirmación positiva de que los paquetes han sido recibidos por el nodo destino mediante un mensaje NA.

- Routing Redirect:

  Estos mensajes permiten a los hosts aprender a través de paquetes de redireccionamiento de ruteo cual es el mejor router a través del cual un nodo externo al enlace puede ser alcanzado. Cuando un host quiere comunicarse por primera vez con un destino sobre una subred a la cual el host no esta conectado directamente, debe elegir un router por default de su Default Router List y mandarle el paquete. El router elegido no es la mejor opción y es forzado a rutear el paquete hacia otro router en el mismo enlace del cual recibió el paquete, así el router elegido además de entregar correctamente el paquete genera un mensaje Routing Redirect para indicar al host que en el mismo enlace un router representa la mejor elección hacia el destino final. Los routers mandan mensajes de redireccionamiento para informar al host de un nodo que puede ser el primer salto en la trayectoria al destino. De esta manera los hosts pueden ser redireccionados a un router que puede ser una mejor opción como primer salto o también pueden ser informados por el redireccionamiento que el destino de hecho es un vecino y actualizan su Destination Cache, el formato de estos mensajes se muestra en la Fig. 3.4.5.3.6:

8	16	32
Tipo=136	Codigo=0	Checksum
Reservado=0		
Dirección de redireccionamiento		
Dirección destino		
Opciones....		

Fig. 3.4.5.3.6 Formato del mensaje de redireccionamiento.

Donde:

- Dirección de redireccionamiento (Target Address): Es la dirección IP que es la mejor opción como primer salto para usarse por la dirección destino ICMP.
- Dirección destino: Es la dirección IP del destino el cual es redireccionado a la dirección de redireccionamiento.

Los problemas ND se relacionan a los enlaces que están dentro de los siguientes tipos:

- Punto a punto: Enlace que conecta dos interfaces, el protocolo ND los maneja como si fueran un caso particular de enlaces multicast.
- Multicast: Enlace de acceso múltiple que puede mandar paquetes a todos los nodos por una sola transmisión de capa de enlace.
- Acceso múltiple sin broadcast (NBMA): Un enlace de acceso múltiple no soporta la transmisión de un paquete a todas las estaciones usando multicast o broadcast, este tipo de enlaces son X.25, Frame Relay y ATM. Únicamente soportan redireccionamiento, detección de inalcanzabilidad de vecino y siguiente salto.
- Medio compartido: Enlace que permite la comunicación directa entre un numero de nodos. Los nodos conectados son configurados sin una lista de prefijos, por lo que los nodos conectados al medio compartido pueden ignorar al vecino, ejemplos de estos medios son SMDS y B-ISDN.

El protocolo ND también maneja las siguientes situaciones:

- Cambio de dirección de capa de enlace. El nodo que sabe que su dirección de capa de enlace ha cambiado manda mensajes NA para actualizar la información en los hosts.
- Balanceo de carga de entrada: Los nodos con diferentes interfaces pueden balancear la carga entre diferentes interfaces en el mismo enlace.

3.4.5.4 DNS

El sistema de nombres de dominio DNS (Domain Name System) usado para realizar la traducción entre nombres y direcciones IP se modifico para incluir un nuevo tipo de registro AAAA para almacenar las direcciones IPv6 que soporta los procesos de búsqueda nombre-dirección y dirección-nombre, para soportar un nuevo dominio que permita realizar las consultas a través de IPv6 y para que los clientes pudieran usar nuevos métodos de consulta para poder procesar las direcciones IPv6.

En el DNS se define un nuevo tipo de registro AAAA, que almacena e indica una sola dirección IPv6. Los registros que el DNS halla en un nodo dependen del protocolo que se esta usando.

- Los nodos que son solamente del tipo IPv4 tienen registros A que contienen direcciones IPv4 en el DNS. Los nodos IPv6 interpretan los contenidos del DNS pre-IPv6 como nodos IPv4. Un nodo IPv6 puede obtener la dirección IPv6 de cualquier nodo IPv4 en el DNS prefijándolo con los 96 bits 0:0:0:0:0:0
- Los nodos que pueden interoperar con nodos solo IPv4 tienen registros AAAA que contienen direcciones IPv6 compatibles con IPv4 y registros A con las direcciones IPv4 equivalentes.
- Los nodos que no pueden interoperar con los que son solo IPv4 tienen registros AAAA con las direcciones solo IPv6.

La petición DNS es posible sobre un transporte IPv4 o un transporte IPv6. Los servidores de nombres deben tener registros AAAA como prerrequisito para usar el DNS con IPv6, esto es por que los nodos IPv6/IPv4 toman decisiones acerca de que protocolo usar basándose en el tipo de dirección IPv6 destino. Los servidores de nombres no tienen que usar necesariamente pilas IPv6 solo tienen que soportar un tipo adicional de registro. Los tipos de registros son:

- Registro AAAA. Este registro que también se conoce como quad A mapea un nombre de host a una dirección IPv6 como lo hace un registro A en IPv4, este registro ha sido designado por el IETF para la resolución de nombre-a-dirección IP, usa el formato: www.6bone.net AAAA 201:5c0:0:2::24.
- Registro A6. Es un registro equivalente al quad A pero establecido como experimental por el IETF, permite el almacenamiento de direcciones IPv6 de una manera jerárquica para simplificar la renumeración de redes usa el formato: www.6bone.net A6 0 201:5c0:0:2::24.
- Registro PTR. El mapeo inverso usado en el proceso de búsqueda dirección IP-a-nombre de host usa el registro PTR. Es equivalente al registro pointer que mapea una dirección-a-nombre de host en IPv4. El dominio de alto nivel para el DNS IPv6 inicialmente era ip6.int, ahora el dominio top-level para direcciones IPv6 es ip6.arpa. Su formato es:

4.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.0.0.c.5.0.1.0.2.0.ip6.arpa PTR www.6bone.net.

- Registros DNAME y Binary Labels. Son unos nuevos registros que permiten la renumeración para el mapeo inverso mas fácilmente.

3.4.5.5 MLD

El protocolo de descubrimiento de oyentes multicast MLD (Multicast Listener Discovery) es usado obligatoriamente en lugar del protocolo IGMP de IPv4 para permitir a los routers IPv6 determinar cuales direcciones multicast son oyentes en cada uno de sus enlaces conectados directamente.
De esta forma los routers escuchan a todos los grupos multicast y realizan el ruteo multicast mediante dos tipos de protocolos de ruteo:

- Protocolos de ruteo en modo denso: DVMRP, PIM-DM, MOSPF.
- Protocolos de ruteo en modo esparcido: CBT, PIM-SM.

3.4.5.6 Protocolos de ruteo

El ruteo en IPv6 se realiza conforme al funcionamiento del ruteo CIDR (Classless Interdomain Routing) de IPv4, es decir usa la correspondencia del prefijo más largo para el anunciamiento de redes o rutas.
IPv6 usa los mismos protocolos de ruteo existentes de IPv4 (IGPs y EGPs) con versiones actualizadas que han sido modificadas para manejar direcciones más grandes:
Protocolos de ruteo interior (IGPs)

- **RIPv6.**
  RIP pasa a ser RIPng este sigue siendo un protocolo usado para redes pequeñas que usa el método de vector de distancia, en el cual cada router manda su vector distancia a los routers adyacentes cada 30 seg. Las tablas de ruteo almacenan solo el mejor siguiente salto hacia cada destino, su principal limitante es que permite un máximo de 15 saltos, ignora las velocidades de los enlaces, su convergencia es lenta en caso de modificaciones de topología de la red, por lo que puede ser usado solamente en redes pequeñas. RIPv6 es la versión de RIP que puede ser usado con IPv6, tiene el mismo funcionamiento que RIP-2 con la diferencia que soporta prefijos, direcciones y el siguiente salto con direcciones IPv6 de 128 bits, sin

agregar nuevas características y sin eliminar los limites citados anteriormente, esto se hace para que RIPv6 pueda ser implementado en dispositivos muy simples sobre los cuales OSPFv6 seria problemático. Los mensajes del protocolo son transportados mediante IPv6 y se usa la dirección multicast FF02::9 para enviar mensajes de actualización a todos los routers RIP. Solamente maneja dos tipos de mensaje Request y Response que son transportados sobre UDP, se limita el numero de destinos por cada paquete para que el paquete IPv6 resultante no exceda el MTU del enlace.

- **OSPFv6.**
  OSPF se basa en el concepto de jerarquía, la raíz de la jerarquía es el sistema autónomo que se subdivide en áreas que contienen a redes interconectadas. Los routers OSPF pueden ser: routers internos, router de limite de área, router backbone o routers internos, router limite del AS.
  OSPF se convierte en OSPFv6 (OSPFv3) que también sigue siendo un protocolo IGP para redes autónomas más grandes y que usa el método de estado de enlace. Esta versión adaptada para manejar direcciones IPv6 incluye los siguientes cambios: es independiente de la plataforma, realiza un procesamiento por enlace mas que por nodo, soporta varias peticiones por enlace, tiene algunos cambios en el formato del paquete y de la autenticación. OSPFv3 usa a IPv6 como transporte de las nuevas direcciones de 128 bits y las longitudes del prefijo asociado. En OSPFv6 las áreas son identificadas pro direcciones de 128 bits. Las direcciones de enlace local (link-local) son usadas como dirección fuente. No se agregaron nuevas funciones a OSPF ya que representa uno de los mejores protocolos IGP.
  OSPFv6 descansa directamente sobre IPv6 y el encabezado OPFv6 es identificado por el valor 89 en el campo next header.

- **IS-IS.**
  IPv6 IS-IS tiene capacidad de ruteo IPv6, ya que comparado con IS-IS se le agregaron: alcanzabilidad IPv6, dirección de interfase IPv6 y un nuevo identificador de protocolo IPv6.

Protocolos de ruteo exterior (EGPs)

- **BGP4.**
  BGP4 es la nueva versión del protocolo de ruteo de frontera BGP el cual interconecta sistemas autónomos grandes. MBGP4 tiene los mismo beneficios de MBGP de IPv4 pero con algunas mejoras como soporte para una familia de dirección IPv6 e información de alcanzabilidad de capa de red (NLRI) y atributos de siguiente salto que usan direcciones IPv6 y direcciones de ámbito (scope). Para el siguiente salto se usa una dirección IPv6 global y mayormente una dirección de enlace local cuando el destino es alcanzable en el mismo enlace.
- **IDRPv2.**
  El protocolo de ruteo interdominio IDRPv2 es un protocolo para ser usado con IPv6. Es un protocolo de vector de ruta derivado de BGP-4. Usa el término dominio de ruteo en lugar de AS, el dominio de ruteo usa un prefijo IPv6 de 128 bits. Los dominios de ruteo se agrupan en confederaciones y son identificadas por prefijos IPv6. La confederación de dominios de ruteo pueden ser agrupados introduciendo

un numero arbitrario de niveles jerárquicos. Cada router calcula su ruteo hacia un destino dado y lo transmite a los routers adyacentes IDRP a través de un vector de ruta. IDRP descansa sobre IPv6 y su encabezado es identificado por el valor 45 en el campo next header.

El ruteo en IPv6 trata las direcciones de una red como un conjunto de identificadores, y cada red requiere una entrada en la tabla de ruteo. El ruteo de IPv6 es casi idéntico al de IPv4, esto se hace con la idea de mantener la actual inversión en protocolos y aplicaciones de Internet.

Gracias a la longitud mayor de las direcciones (128 bits) las tablas de ruteo se pueden reducir ya que se tienen mas niveles de jerarquía y como consecuencia mas eficiencia con menos memoria.

Las extensiones de ruteo soportan nuevas funcionalidades de ruteo:

1. Selección de proveedores. Opción que permite a la maquina origen listar los nodos intermedios necesarios para alcanzar el destino. Esta opción viene en la base de la seguridad, prestaciones y costo.
2. Maquinas móviles. También llamadas plug and play. Esta función permitirá conectar una maquina a la red sin necesidad de configuraciones manuales con configuración automática y actualización de las tablas.
3. Redirección automática. El destino puede responder a la dirección origen invirtiendo la secuencia de direcciones, eliminando así el proceso de ruteo.

Relación entre el direccionamiento y el ruteo.

En IPv4 no existe una relación entre direcciones y topología, las direcciones son directamente asignadas a usuarios finales, los routers del núcleo de Internet mantienen en sus tablas de ruteo una entrada por cada red conectada al Internet, por lo que las tablas tienden a explotar con el crecimiento del Internet, ni con la introducción de CIDR para agrupar anunciamiento de direcciones contiguas se pueden tener muchos beneficios debido a la filosofía de asignación de direcciones IPv4.

Por lo anterior IPv6 cambia de un esquema basada en la asignación de direcciones para usuarios finales a un esquema basado en proveedor. Con este nuevo esquema a cada proveedor se le asigna un conjunto de direcciones que es dividido en conjuntos más pequeños para ser asignados a sus usuarios, la longitud mayor de la dirección IPv6 puede contener este nivel de jerarquía. Los routers del ISP tienen una sola entrada por cada red dentro del ISP, una entrada por default hacia el upstream (proveedor superior) y anuncian su conjunto de direcciones al upstream con una sola entrada. Los routers del núcleo reciben solamente una entrada que agrupa todas las direcciones de los ISPs, por lo que el tamaño de las tablas de ruteo es proporcional al numero de proveedores no al numero de redes.

Ruteo Multicast

El ruteo multicast se refiere al ruteo de paquetes cuya dirección destino es una dirección multicast, esto es la dirección de un grupo de estaciones. Las direcciones multicast se asocian con grupos predefinidos y tienen significado con respecto al nodo o al enlace, mientras que otros grupos pueden tener miembros en varias partes de la red Internet, por lo que los paquetes direccionados a estos grupos multicast deben ser ruteados por routers. El protocolo de administración de miembros multicast IGMP se volvió parte integral de ICMPv6. El protocolo de ruteo de paquetes multicast MOSPF se volvió parte integral de OSPFv6.

Para rutear paquetes multicast, se debe crear un árbol de distribución (multicast tree) para alcanzar a todos los miembros del grupo, el árbol es dinámico por que nuevos miembros pueden anexarse o los existentes pueden dejarlo en cualquier momento. El problema de ruteo multicast se vuelve parte integral de IPv6 por medio de ICMPv6 y OSPFv6.

Servicios
La versión IPv6 debe seguir ofreciendo los mismos servicios de IPv4 asi como servicios adicionales ofrecidos entre los cuales los más importantes son calidad de servicio, seguridad, movilidad.

3.4.5.7 Calidad de servicio

El concepto de calidad de servicio es otra de las características fuertes de IPv6. La calidad de servicio es la entrega confiable de datos sin perdida, sin retardo, sin fluctuaciones (jittering) y con el aseguramiento del ancho de banda. Si una red garantiza alguno de los parámetros capacidad mínima (Mbps), retardo máximo (mseg), fluctuación máxima del retardo o jitter (mseg) o porcentaje máximo de paquetes perdidos se dice que es una red que ofrece calidad de servicio QoS, de lo contrario es una red con servicio best effort.
El servicio es cualquier cosa que se ofrezca al usuario, ya sea de comunicación, de transporte o de aplicación. Esta calidad de servicio medirá el comportamiento de una red con respecto a algunas características de servicios definidos.
Al ser IPv6 el protocolo de comunicación básico en Internet que se basa no en el aseguramiento del ancho de banda requerido por aplicaciones criticas sino en el concepto del mejor esfuerzo y debido a la tendencia de llegar a la convergencia del trafico de voz, datos y video por Internet, IPv6 busca ofrecer una calidad de servicio que apoye esa convergencia y el transito de aplicaciones en tiempo real.
Para ofrecer esta calidad de servicio primeramente el campo tipo de servicio de IPv4 se dividio en dos campos, el primer campo de tres bits indicaba la prioridad y el segundo campo de 4 bits indicaba cinco opciones de tipo de servicio:

- Cuando el campo vale 1000 significa minimizar el retraso.
- Cuando el campo vale 0100 significa maximizar la velocidad.
- Cuando el campo vale 0010 significa maximizar la fiabilidad.
- Cuando el campo vale 0001 significa minimizar el costo.
- Cuando el campo vale 1111 significa maximizar la seguridad.

Existen dos posibles estrategias para proporcionar un trato especial al trafico de usuario en una red:

- Reserva: A veces se le conoce como QoS hard. Estrategia para reservar capacidad para uso exclusivo del usuario. Esta estrategia derrocha recursos en algunos casos pero da una garantía casi total para lo que requiere que cada nodo intermedio recuerde las sesiones activas.
- Prioridad: También llamada QoS soft. Dar mayor prioridad a un usuario que a otros. Esta estrategia aprovecha mejor la infraestructura garantizando el servicio en base a factores estadísticos y los nodos intermedio no necesitan conocer las conexiones activas.

Las dos estrategias son compatibles.
Estos dos mecanismos de calidad de servicio se han desarrollado y estandarizado por el IETF:

- **Los servicios integrados (Int-Serv).**
  Proporcionan un servicio un tanto fino (manejan flujos) y cuantitativo (como la cantidad de bits por segundo), este enfoque usa la señalización del protocolo de reservación de recursos RSVP (Resource Reservation Protocol). El usuario solicita por anticipado los recursos que necesita, cada router de la ruta implementa medidas para satisfacerle. Los servicios que proporciona Int-Serv son:

➢ Servicio Best-Effort que no proporciona ninguna garantía de calidad de servicio.
➢ Servicio Controlled-Load que proporciona una calidad similar a la de una red de datagramas poco congestionada.
➢ Servicio Garantizado, garantiza el caudal y retardo en cada uno de los elementos en la ruta.

El protocolo RSVP no es un protocolo de ruteo, reserva la capacidad solicitada en todos los routers de la ruta en base a una señalización como la usada en una llamada telefónica. Los routers que implementan RSVP manejan cuatro elementos:

➢ Admisión Control: Para comprobar si la red tiene los recursos suficientes para satisfacer la petición.
➢ Policy Control: Para determinar si el usuario tiene los permisos adecuados para la petición que solicita.
➢ Packet Classifier: Clasifica los paquetes en categorías de acuerdo con la QoS a la que pertenecen.
➢ Packet Scheduler: Organiza el envío de paquetes dentro de cada categoría.

Cada router que usa RSVP debe mantener el detalle de todas las conexiones activas que pasan por el y los recursos que cada una ha reservado, es decir el router mantiene información de estado sobre cada flujo. Si no se pueden asegurar las condiciones pedidas se rechaza la llamada.

- **Los servicios diferenciados(Diff-Serv).**
  Proporcionan un servicio menos fino (manejan clases) y cualitativo (como la prioridad mas alta). En lugar de distinguir flujos individuales clasifica los paquetes en categorías. El usuario solicita un determinado caudal en una categoría dada mediante un nivel de prioridad. Los routers tratan cada paquete según su categoría especificada en la cabecera del paquete, van agregando las demandas de los usuarios y propagándolas por la ruta, lo que da la confianza al usuario de obtener la QoS solicitada. Los servicios que proporciona Diff-Serv son:

➢ Servicio Best Effort básico sin prioridad.
➢ Servicio Best Effort con prioridad.
➢ Servicio Assured Forwarding es un servicio similar al de una red poco cargada (Controlled Load) de Int-Serv. Maneja varios niveles de prioridad posibles.
➢ Servicio Expedited Forwarding o Premium es un servicio similar al servicio garantizado de Int-Serv.

El Policy Control/Admission Control solo se efectúa en los routers de entrada a la red y en los que atraviesan fronteras entre redes diferentes.

Soporte de IPv6 para Int-Serv.
El campo etiqueta de flujo especifica flujos que necesitan calidad de servicio especial.
El concepto de flujo solamente es aplicado a protocolos no orientados a conexión o de datagramas.

En forma genérica un flujo es un trafico continuo unidireccional de datagramas relacionados que se produce como resultado de una acción del usuario y requiere una misma QoS. Los flujos se pueden agrupar en clases y los grupos dentro de una misma clase recibirán la misma QoS.
IPv6 define el flujo como una secuencia de paquetes en alguna forma correlacionados (generados por la misma aplicación) enviados desde un origen particular a un destino particular y que por lo tanto deben ser coherentemente tratados por la capa IP.
Los paquetes pueden pertenecer al mismo flujo sobre la base de parámetros como la dirección fuente, la dirección destino, la QoS, la autenticación y la seguridad.
La etiqueta de flujo marca los paquetes que pertenecen a un mismo flujo. Cada fuente selecciona sus propios valores de etiqueta de flujo.
Cada router en la ruta identifica los datagramas que corresponden al flujo para el que se ha hecho la reserva.
En IPv4 la identificación de flujos se realiza a partir de las direcciones origen y destino y el numero de puerto (TCP o UDP) de origen y destino.
En IPv6 los ruteadores usan la etiqueta de flujo (en lugar de números de puerto) mas las direcciones fuente y destino para identificar flujos distintos. Los ruteadores almacenan esa etiqueta asociándola a la sesión establecida entre dos nodos, con lo que los ruteadores procesaran los paquetes del flujo de esa sesión mas eficientemente verificando únicamente la etiqueta y aplicaran el concepto de conmutación de etiquetas para no analizar todo el encabezado ni las tablas de ruteo.
Se usa un valor de cero para la etiqueta de flujo cuando no se requiere una QoS especial.

Soporte de IPv6 para Diff-Serv.
Las categorías de Diff-Serv se identifican mediante el campo DS, en IPv4 el campo DS sustituye al Tipo de Servicio.
Para IPv6 inicialmente se especifico un campo prioridad de 4 bits seguido del campo etiqueta de flujo de 24 bits. Posteriormente estos se cambiaron para formar el campo clase de trafico de 8 bits y el campo etiqueta de flujo de 20 bits. El reciente concepto de servicios diferenciados DS (DiffServ) vuelve a utilizar los campos clase de trafico de IPv6 y tipo de servicio de IPv4.
De esta forma en IPv4 el campo Tipo de Servicio=Diff-Serv y en IPv6 el campo Clase de trafico=Diff-Serv.
El campo servicios diferenciados se divide en dos campos, de los cuales el segundo es para uso futuro y el primero llamado DSCP (DiffServ CodePoint) de seis bits de longitud define los comportamientos que puede tener un paquete. Con 6 bits en el campo DS se pueden tener hasta 64 codepoints (categorías de trafico diferentes).
El campo de 8 bits clase de trafico especifica clases de paquetes que necesitan calidad de servicio especial al igual que el campo tipo de servicio de IPv4. Este campo puede ser inicializado por la fuente o por un router en la ruta y puede ser reescrito por un router en la ruta.
El concepto de servicios diferenciados tiene en cuenta que al ser IPv6 un protocolo de mejor esfuerzo no puede garantizar una calidad de servicios total por lo que puede tratar los paquetes en forma diferenciada, es decir según la prioridad con la que estén marcados los paquetes serán los primeros o últimos en ser descartados por los ruteadores en caso de congestión.

Se usa un valor de cero para el campo clase de trafico cuando no se requiere una calidad servicio especial.
Concretamente la calidad de servicio realiza una diferenciación entre trafico y tipo de servicio, ya que los usuarios pueden manejar diferentes clases de trafico a la vez diferentemente.

3.4.5.8 Seguridad

Existen tres principales preocupaciones relativas a la seguridad en las redes:

- **Confidencialidad de los datos.**
  La preocupación de la confidencialidad es mantener los datos ocultos y seguros. Por ejemplo se desea que información importante de las compañías, bancos en línea o información de tarjetas de crédito, se mantenga segura de gentes ajenas a ella, para que así, si alguien captura el datagrama con dicha información la información debería parecerles sin sentido. Un método para asegurar la confidencialidad de la información es el uso de la encripción.
  Encripción.
  La encripción es un esquema que toma los datos de usuario referidos como texto plano y lo convierte a datos secretos o ilegibles llamados texto cifrado (ciphertext). Para realizar el cifrado del texto (encripción) se requiere un algoritmo de encripción.
  Algoritmo de encripción.
  Un mensaje es introducido en un algoritmo de encripción y la salida es el texto cifrado. Asimismo el texto cifrado es alimentado en un algoritmo de desencripción para regresar a los datos originales. El algoritmo de encripción a su vez requiere una llave de encripción.
  Llave de encripción.
  Una llave de encripción es una cadena de bits que es usada para controlar la salida del texto cifrado del algoritmo de encripción.
  Para desencriptar el texto cifrado, la otra parte debe conocer que algoritmo y llave de encripción fueron usados para encriptar los datos. La forma de intercambiar la información entre los extremos (algoritmo y llave) debe ser una forma segura ya que por métodos tradicionales (teléfono, correo, mensajero) son inseguros por sí mismos. La llave secreta de encripción no es cambiada muy a menudo a menos que se tenga que cambiar. Existen dos tipos encripción:
  Encripción simétrica.
  Es la forma más directa de encriptar con la menor cantidad de sobreencabezado. La encripción simétrica usa la misma llave para la encripción y el desencriptamiento, la misma llave debe ser conocida en ambos extremos. Es la forma más rápida de encripción, por lo que es usada para encriptar grandes cantidades de datos.
  Encripción asimétrica o encripción de llave publica.
  Usa llaves diferentes para la encripción y desencriptamiento. Para su implementación usa un par de llaves publicas y privadas, una llave será usada para encriptar y una llave diferente será usada para desencriptar. Computacionalmente es más lenta que la encripción simétrica, por lo que es perfecta para verificar pequeñas cantidades de datos, tales como firmas digitales. Las firmas digitales son usadas para validar que eres quien dices ser.
  Algoritmos de encripción:

DES

El algoritmo de encripción de datos estándar DES (Data Encrytion Standard) es uno de los primeros estándares para encripción, fue desarrollado por IBM, también es llamado DEA y DEA-1, es un algoritmo de llave simétrico que encripta datos en bloques de 64 bits mediante una llave de 56 bits. Tiene cuatro modos de operación: ECB, CBC, OFB, CFB, de los cuales CBC es el mas usado. Los cuatro modos de operación permiten la encripción sobre enlaces satélite y la encripción de un carácter a la vez.

En el modo de operación de encadenamiento de bloques cifrados CBC (Cipher Block Chaining), encripta bloques dc datos de 64 bits, la información de un bloque de 64 bits de datos encriptados es usada para modificar la encripción del siguiente bloque, es decir el texto cifrado del bloque previo es realimentado en la encripción del bloque actual.

DES puede ser hackeado en muy poco tiempo, debido a la longitud de su llave, puesto que entre mas larga es la longitud de una llave más grande es el numero de posibles salidas encriptadas para un mensaje dado. Otros algoritmos como 3DES o AES ofrecen una seguridad mayor.

3DES

El algoritmo tripe DES es un estándar de encripción mejorado, también es llamado modo de encripción-desencripción-encripción (EDE). La encripción triple DES ejecuta al algoritmo simple DES tres veces con tres llaves diferentes, la llave sigue siendo de 56 bits.

Transmisor (EDE):

- Encripta con DES y la primer llave.
- Desencripta con DES y la segunda llave.
- Encripta con DES y la tercer llave.

Receptor (DED):

- Desencripta con DES y la primer llave.
- Encripta con DES y la segunda llave.
- Desencripta con DES y la tercer llave.

Computacionalmente es más extenso que DES por lo que podría ser mas seguro.

AES

El estándar de encripción avanzado AES (Advanced Encryption Standard) es un nuevo estándar de encripción que reemplaza a DES, proporciona longitud de s llave de 128, 192 y 256 bits. El algoritmo que usa es Rijindael. El algoritmo es conocido como un algoritmo de cifrado de bloques donde cada bloque y llave pueden ser de 128, 192 o 256 bits de longitud.

La encripción no asegura la integridad de los datos.

- **Integridad de datos.**

Asegurar que los datos no han sido cambiados. Aunque la información puede ser asegurada y oculta (encripción) para que nadie pueda determinar o entender su contenido conforme atraviesa el Internet, esta podría ser cambiada, por lo que tenemos que asegurarnos que los datos no son modificados a lo largo del camino.

El hacker al no poder crackear el algoritmo de encripción y la llave, podría provocar estragos modificando algunos bits (corrompidos) que son transportados en la carga útil encriptada, por lo que los datos (salida desencriptada) al llegar al otro extremo,

no serán los que originalmente se mandaron a través de la red. La pregunta de esta preocupación es ¿Cómo asegurarse de que si los datos han sido modificados que el host remoto reconozca esto y rechaze procesar la información? Un método para mantener la integridad de los datos es el uso de algoritmos hashing.

Hashing.

Un hash es similar a una suma de comprobación CRC (checksum). Un algoritmo hash de una dirección es una representación o resumen del mensaje y no contiene al mensaje, ya que toma una entrada de longitud variable y la convierte en una salida hash de longitud fija mas pequeña y se anexa a la información. A partir de la salida hash no se puede determinar la entrada original.

En forma general su funcionamiento es como sigue: antes de transmitir los datos, el procedimiento hashing produce una salida hash de longitud fija conocida como hash o finger print. El hash se pone en un campo del paquete junto con los datos y se transmiten sobre la red. El destino tomas los datos y mediante el algoritmo hashing calcula su propio hash y lo compara con el hash transportado en el paquete, si son iguales se esta verificando con ello que los datos no fueron modificados, si no corresponden el paquete se desecha.

Los algoritmos hashing de una sola dirección pueden usar la operación modulo en la creación del hash. Las funciones hashing deben ser tan libres de colisiones como se pueda. Una colisión hash es cuando dos mensajes diferentes tienen la misma salida hash. Algunos algoritmos hashing son el MD5 y SHA.

MD5

El algoritmo hashing MD5 (Message Digest) produce una salida hash de 128 bits.

SHA

El algoritmo hashing SHA (Secure Hash Algoritm) produce una salida hash de 160 bits. Este algoritmo es más seguro que MD5 por que es menos propenso a tener colisiones. Por su salida hash más larga puede producir muchas más combinaciones. Sin embargo requiere de mas calculo.

- **Autenticación de los datos.**

Es una validación o verificación de que los datos provengan del host (fuente) del que se esperaba vinieran. Un método de validar los datos es autenticar al transmisor. La autenticación busca evitar que en algún proceso de comunicación se mande información critica al receptor equivocado. Los datagramas se validan para verificar que vengan de la fuente apropiada.

El método hashing solo verifica que los datos no sean cambiados pero no valida que la información venga de la fuente apropiada. Los algoritmos MD5 y SHA no se pueden usar solos, por lo que necesitan ser hasheados con una llave secreta no conocida por nadie más. La llave es hasheada junto con los datos (el datagrama entero junto con la llave es hasheado), esto no significa que la llave es transmitida junto con los datos (el datagrama no transporta la llave). Para que los hashes correspondan el extremo remoto deberá conocer la llave antes de que ejecute sus algoritmos hashing. La llave precompartida es usada para verificar que la información venga de la fuente esperada. El proceso de autenticación usa HMAC.

HMAC.

El código de autenticación de mensaje hashing HMAC (Hashing Message Authentication Code) es un algoritmo que usa un algoritmo hashing (MD5 o SHA)

con una llave secreta. Las llaves secretas deben ser compartidas antes de checar la autenticación. Realiza la operación sobre un mensaje de longitud variable junto con una llave y regresa un valor de longitud fija.
Para HMAC con MD5 (integridad+autenticación) una llave de 16 bytes es usada.
Para HMAC con SHA (integridad+autenticación) una llave de 20 bytes es usada.
Con el datagrama original y la llave secreta el destino calcula el hash, si corresponde con el del datagrama, se acepta, si no, se desecha por que pudo ser originado desde una fuente desconocida que no conoce la llave o pudo ser modificado en el camino.

IPSec

IPSec (IP Security) es un conjunto de protocolos que proporcionan servicios de seguridad para el trafico IP.
La seguridad del protocolo de Internet IPSec sienta las bases para usar la seguridad en el protocolo IP, para ello define un conjunto de protocolos que proporcionan servicios de seguridad para el trafico en la capa IP (capa 3 del modelo OSI). Los protocolos usan los algoritmos que proporcionan seguridad como: algoritmos de encripción (DES, 3DES, AES), algoritmos de autenticación (MD5, SHA) y los algoritmos de validación (HMAC).
IPSec se basa en dos protocolos para proporcionar seguridad: ESP y AH.

ESP.

El protocolo de encapsulamiento de seguridad de la carga útil ESP (Encapsulating Security Payload) proporciona confidencialidad del flujo de trafico (DES, 3DES, AES), integridad no orientada a conexión, autenticación del origen de los datos y servicio anti-replica (MD5 y SHA).
Con el uso de la encripción ESP se ejecutan hashing y autenticación al mismo tiempo, en lugar de tener que implementar cada uno de los algoritmos por separado.
ESP no usa el servicio de un protocolo de transporte por que funciona directamente por encima de IP con el numero de protocolo 50. Puede funcionar en modo túnel o modo transporte.
En modo túnel el encabezado ESP es insertado antes del encabezado IP original y un nuevo encabezado IP (encabezado de túnel) es insertado enfrente del encabezado ESP. La encripción y autenticación se aplica al datagrama IP original entero, el encabezado del túnel no es encriptado ni autenticado, Fig. 3.4.5.8.1.

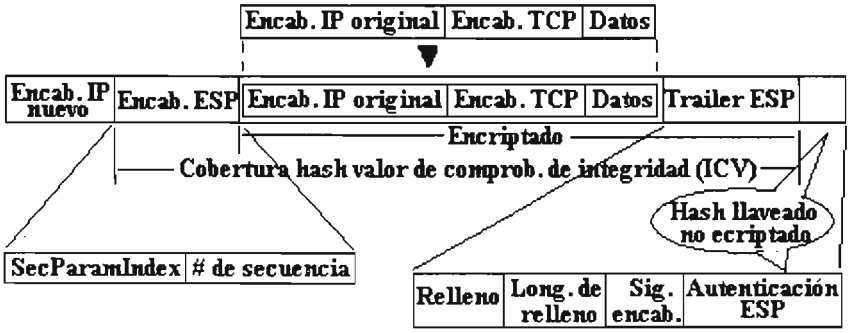


Fig. 3.4.5.8.1 Transformación de un paquete IP por encapsulamiento ESP-túnel.

La Fig. 3.4.5.8.1 muestra la operación de ESP, donde se observa que el datagrama IP se encapsula entre un encabezado ESP y un trailer ESP. El encabezado ESP y el datagrama IP son hasheados, lo que no ocurre con el nuevo encabezado IP o encabezado del túnel. Algunos de los campos de proceso ESP son:

- SecParamIndex.
  Es el índice de parámetros de seguridad (SPI), ya que en IPSec cada VPN es identificada por su SPI, este parámetro es un índice en una base de datos de asociaciones de seguridad. La base de datos contiene la lista de VPNs y sus parámetros asociados como algoritmos de encripción y hasheo para las VPNs.
- # de secuencia.
  Este es un numero de 32 bits que funciona como un contador. Cuando el túnel se establece su valor inicial es cero, así el primer paquete es transmitido con numero de secuencia 1, el siguiente con 2 y así sucesivamente.
- Relleno.
  Son bits introducidos por el algoritmo de encripción
- Next header.
  Indica el tipo de datos encapsulados en la carga útil.
- Autenticación ESP.
  Es el valor no encriptado que se transmite para verificar la autenticidad antes de desencriptar.

ESP cuando funciona en modo túnel hace dos funciones: encripta los datos (no encripta el encabezado del túnel) del datagrama original con algún algoritmo de encriptamiento (DES, 3DES, AES) y autentica los datos (no autentica el encabezado del túnel) mediante un algoritmo de autenticación (HMAC_MD5, HMAC_SHA) para checar el datagrama original y el encabezado ESP.

AH

El protocolo de autenticación del encabezado AH (Authentication Header) tiene el numero asignado 51, no hace ninguna encripción solamente verifica la integridad no orientada a conexión, autenticación del origen de los datos y servicio anti-replica (MD5 y SHA).
En modo túnel realiza la autenticación mediante los algoritmos HMAC_MD5 y HMAC_SHA. Este protocolo si autentica el datagrama entero incluyendo el encabezado del túnel, la Fig. 3.4.5.8.2 muestra el proceso de autenticación con AH.

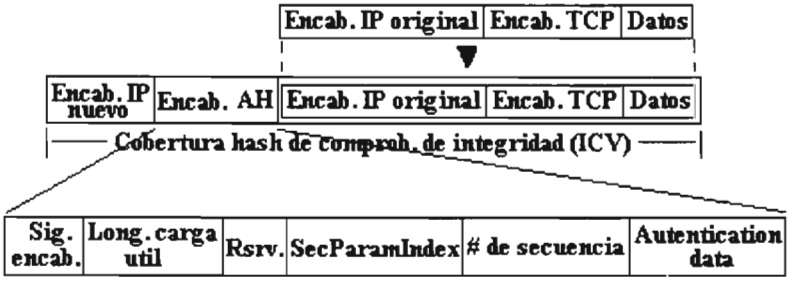


Fig. 3.4.5.8.2 Transformación de un paquete IP por la autenticación AH en modo túnel.

AH autentica el datagrama entero, los campos que cambian de valor por el proceso de ruteo como el campo TTL valen cero para el calculo hash.

Asociaciones de seguridad.
Las asociaciones de seguridad SA (Security Association) completan el ambiente IPSec. Una AS es un acuerdo entre dos entidades que se comunican, que intercambian información como los protocolos de encriptación y autenticación (ESP o AH), funcionamiento en modo túnel o transporte, llaves, el SPI (Security Parameter Index) que debe ser único para cada túnel, la dirección IP destino. Las AS identifican conexiones simples, las conversaciones bidireccionales requieren dos AS, ya que se requiere una AS para el trafico de salida y otra para el trafico de entrada. El SPI puede ser el mismo en ambos extremos del túnel o diferente.

Intercambio de llaves IKE
Con las VPNs manuales se deben intercambiar varios datos antes de configurar los túneles, eso es útil cuando se tienen algunos cuantos túneles configurados, pero cuando ya se tienen demasiados túneles y las llaves deben ser cambiadas constantemente, el trabajo que implica es pesado.
El protocolo para el intercambio de llaves por Internet IKE (Internet Key Exchange) se creo para intercambiar la información de una forma segura y dinámica con poca intervención.
IKE establece las AS creando túneles VPN IPSec sobre Internet, negocia las propuestas que contienen los algoritmos de encripción y autenticación, crea las llaves de encripción y autenticación automáticamente y tiene la capacidad de renovarlas frecuentemente. Para su funcionamiento IKE se basa en el algoritmo Diffie-Hellman.

Algoritmo Diffie-Hellman.
Diffie-Hellman (DH) es el algoritmo principal de IKE para el intercambio de llaves, con el, dos dispositivos que se están comunicando en los extremos del túnel VPN crean un par de llaves publicas/privadas únicas y se intercambian solo las porciones publicas del par de llaves, Fig. 3.4.5.8.3.

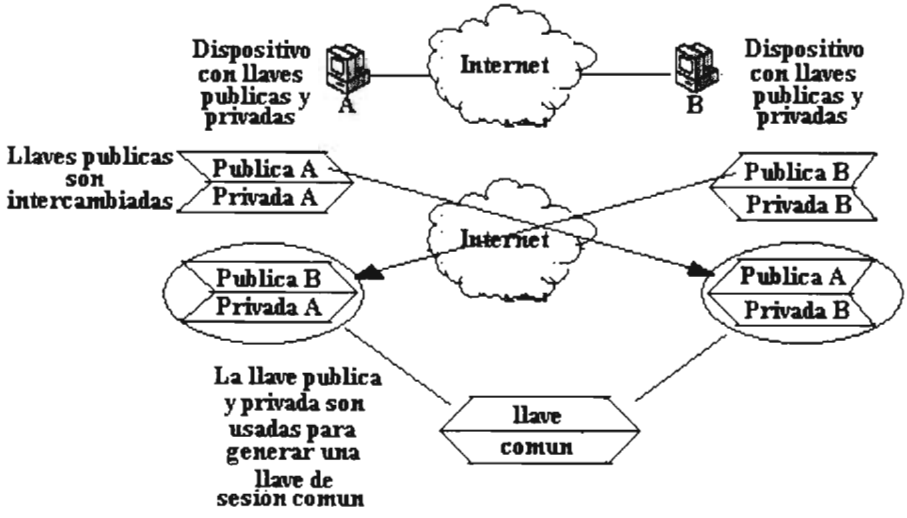


Fig. 3.4.5.8.3 Intercambio de llaves mediante el algoritmo DH.

La llave publica es mandada en texto plano sobre la red, con esa llave publica los dispositivos generan una llave de sesión común (mediante el algoritmo DH) usada por los algoritmos de encripción simétrica. Esa llave de sesión es un valor secreto compartido.

La ventaja del algoritmo DH se debe a que los extremos crean el valor secreto a través de un medio inseguro y sin tener que transmitir el valor secreto, además de que es imposible generar su origen a partir del valor secreto.
El algoritmo Diffie-Hellman realiza sus cálculos en base a 5 conjuntos de números primos muy grandes y un generador que se pueden usar en conjunto con la función modulo. Los grupos Diffie-Hellman son representaciones de respuestas matemáticas gigantescamente enormes. Existen 5 grupos Diffie-Hellman que se derivan del uso de números primos muy grandes.
Los grupos DH usan un numero primo m (numero primo de determinados bits) y un generador (g). El grupo DH 1 usa un p=768 bits y un g=2, el grupo DH 2 un p=1024 bits y g=2, el grupo DH 5 usa un p=1536 bits y un g=2. La llave de sesión común se genera al aplicar a la llave privada la función $g^k \text{mod } P$.
Entre más grande es el modulo más segura es la llave generada, sin embargo el desempeño puede decrementarse por el proceso mas largo que toma la generación de la llave. Todo el proceso IKE se ejecuta en dos fases: fase 1 y fase 2.

Fase 1 de IKE
La fase 1 también conocida como IKE gateway establece un canal seguro entre los gateways para que se puedan realizar las negociaciones de la fase 2. En esta fase se negocian los algoritmos de encripción y autenticación. Usa el algoritmo DH para generar una llave simétrica común a los extremos. La información intercambiada en la fase 2 usara los algoritmos de encripción y autenticación y las llaves de la fase 1.
La fase 1 puede funcionar en dos modos: modo principal y modo agresivo. El modo principal es usado en configuraciones donde la dirección IP es estática, este modo intercambia entre sus primeros mensajes la dirección IP, por lo que no se puede usar en ambientes dial-up. El modo agresivo es usado en implementaciones dial-up donde la dirección IP es asignada dinámicamente.

Fase 2 de IKE
La fase 2 es llamada una VPN establece un túnel seguro para la comunicación de red a red. Crea una AS (acuerdo de algoritmos, SPIs y llaves) de fase 2 usando el canal seguro de fase 1. Los algoritmos de encripción y autenticación seleccionados serán usados para encriptar y autenticar los datos de usuario

IPv6 ofrece el servicio de seguridad de la información a nivel de red, al ser establecido como obligatorio el soporte de IPsec en IPv6, IPv6 puede ofrecer seguridad del contenido de la información de extremo a extremo por medio del estándar de seguridad IPsec. Por lo que se puede encriptar cualquier tipo de información contenida en los paquetes IPv6.
IPSec se diseño para proporcionar seguridad criptográfica de alta calidad e interoperable tanto en IPv4 como en IPv6.
La seguridad en IPv6 deberá ofrecer servicios de confidencialidad e información y de flujo, autenticación y protección contra reenvios a través de tres protocolos básicos soportados por IPSec:

- **Autenticación del encabezado.**
  Solamente autenticación mediante el protocolo de autenticación de encabezado AH (Authentication Header).
- **Encapsulamiento de la carga útil.**

Encapsulamiento de la información mas autenticación mediante el uso del protocolo de encapsulamiento de seguridad de la carga útil ESP (Encapsulation Security Payload).

- **Intercambio de llaves por Internet.**
  Administración del intercambio de llaves manualmente o automáticamente mediante protocolos de intercambio de llaves a través de Internet IKE (Internet Key Exchange).

3.4.5.8.1 Autenticación IPv6

El encabezado AH se compone de una parte fija de 64 bits seguida de un numero variable de bloques de 32 bits, Fig. 3.4.5.8.1.1

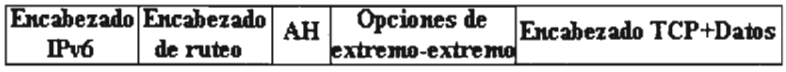


Fig. 3.4.5.8.1.1 Uso del encabezado de autenticación.

La parte variable del encabezado de autenticación consiste de un numero variable de bloques de 32 bits que contienen los datos de autenticación, por lo que la longitud del encabezado de autenticación depende de algoritmo de autenticación, Cuando un nodo recibe un paquete con un encabezado AH la integridad y autenticidad del paquete debe ser checada, para esto primero se debe normalizar el paquete recibido, eliminando las partes variables y correctamente calculando el valor de autenticación de las partes variables.
La integridad de los sistemas de telecomunicaciones normalmente es garantizada calculando y checando el valor de una función apropiada de los datos, normalmente llamados Message Digest (MD).
Los algoritmos CRC-16 y el CRC-32 protegen los datos de ser modificados por errores aleatorios pero fallan para modificaciones deliberadas. Un mayor grado de seguridad es proporcionado con mejores algoritmos como el MD5 y el SHA, estos algoritmos digest checan la integridad de los datos y su autenticidad, aplicando algunos parámetros que prueban la identidad del remitente simultáneamente, mediante el uso de algoritmos de encripción de llaves publicas.
La técnica de autenticación usada por IPSec es llamada keyed MD5, esta usa para el calcular el digest MD5 una llave que consiste de una cadena de bits secretos.
También se ha propuesto la técnica keyed-SHA que se basa en el algoritmo message digest SHA, que tiene mejores propiedades de seguridad que MD5 por que produce un digest de 160 bits mayor que un digest de 128 bits.

3.4.5.8.2 Encapsulamiento(encriptamiento) IPv6

El protocolo de encapsulamiento de la carga útil oculta los datos del nivel superior y todos los siguientes encabezados, Fig. 3.4.5.8.2.1.

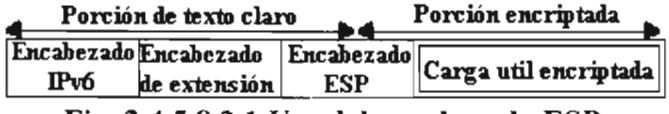


Fig. 3.4.5.8.2.1 Uso del encabezado ESP.

El encabezado ESP consiste de un numero entero de bloques de 32 bits, donde el primer bloque contiene el SPI que selecciona la SA a ser usada en el descifrado de todos los otros bloques en el paquete.
El formato exacto de la parte encriptada depende del algoritmo de encripción usado. La técnica de encripción por default en IPv6 es DES-CBC, es decir el algoritmo DES aplicado en modo de encadenamiento de bloques cifrados CBC (Cipher Block Chaining).
DES es un algoritmo de encripción de llave privada que se aplica a bloques de datos de 64 bits con una llave de 56 bits (se puede extender a 64 bits agregando un bit de paridad por cada 7 bits de la llave). El modo CBC divide el flujo de datos en una secuencia de bloques de 64 bits y cada bloque es EX-Ored con el resultado de la encripción previa antes de ser encriptado. La encripción del primer bloque de datos requiere un valor inicial llamado vector de inicialización IV (Initialization Vector). Este valor no debe ser nulo y seleccionado para insertar un factor aleatorio en el proceso de encripción. El valor del IV puede ser un numero de 64 bits generado por un generador de números pseudo-aleatorios o el valor de un numero de 32 bits generado en una forma similar y que es extendido a 64 bits concatenándolo a su complemento. En el modo DES-CBC la porción encriptada del encabezado ESP comienza con un IV compuesto de un numero entero de palabras de 32 bits. También su longitud depende de la SA, pero se han especificado IV de 32 y 64 bits. El IV es seguido de la carga útil encriptada que se rellena con bloques para tener un encabezado múltiplo de 64 bits. La longitud mínima del relleno varia entre 0 y 7 bytes pudiendo ser de hasta 255 bytes.
El algoritmo DES-CBC debe ser disponible en las implementaciones estándar IPv6, ya que es considerado como un algoritmo moderadamente difícil de ser hackeado. También se ha propuesto el algoritmo 3DES-CBC que plica la operación repetida de la transformación DES al mismo bloque de datos con tres llaves diferentes y es criptográficamente mas fuerte que el DES por que es equivalente a un algoritmo de encripción que usa una llave de 112 bits que es mayor a la llave de 56 bits usada por DES.
Con el uso de IPSec se pueden proteger una o varias rutas de información, o se puede proteger la ruta entre dos nodos, entre un par de gateways de seguridad, o entre un nodo y un gateway de seguridad, Fig. 3.4.5.8.2.2.

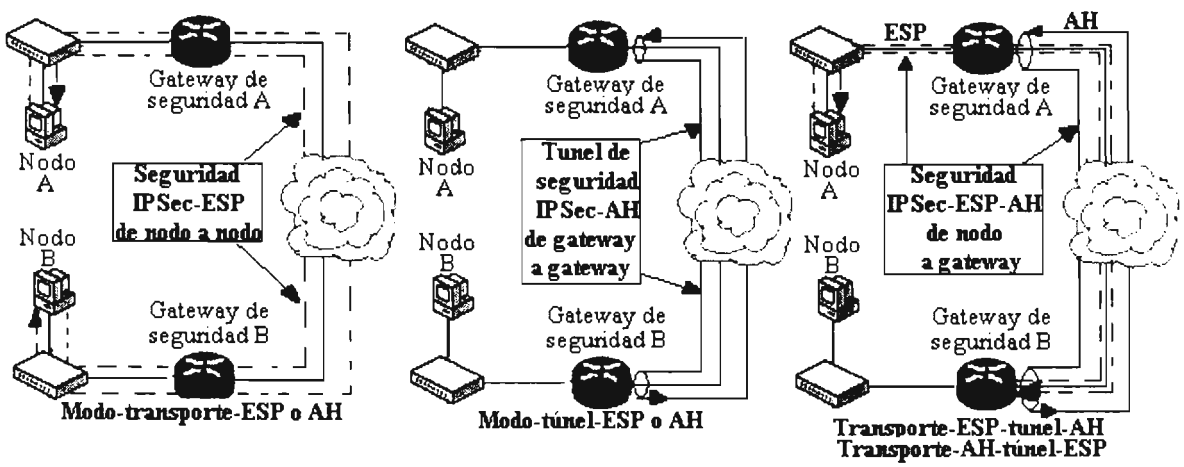


Fig. 3.4.5.8.2.2 Seguridad IPSec entre nodos y gateways de seguridad.

La Fig. 3.4.5.8.2.2 nos muestra que ambos protocolos ESP y AH pueden trabajar en dos modos:

- Modo transporte.
  Este modo puede ser usado entre sistemas finales o intermedios siempre y cuando ambos extremos soporten IPSec.
- Modo túnel.
  Este modo de operación encapsula básicamente paquetes IP inseguros entre sistemas intermedios no entre nodos finales.

IPSec usa el concepto de asociaciones de seguridad SA (Security Association) para crear los grupos de parámetros bidireccionales que controlaran la seguridad en los extremos de la implementación, tanto en AH como en ESP. Ambos protocolos explotan las SA para estar de acuerdo en los algoritmos de seguridad y parámetros entre el transmisor y el receptor. Cada nodo IPv6 administra un conjunto de SA, una por cada comunicación activa. Cada asociación de seguridad contendrá en cada extremo cuatro datos básicos:

- Índice de seguridad. El índice de seguridad SPI (Security Parameter Index) es un conjunto de bits que se asignan a una asociación de seguridad y que apunta a la base de datos de políticas de seguridad SPD (Security Policy Index). El SPI es un parámetro contenido tanto en el encabezado AH como en el ESP que especifica cual SA es usada para desencriptar y/o autentificar el paquete. En la comunicación unicast el SPI es elegido por el destino y regresado al remitente cuando la comunicación es establecida. En transmisiones multicast el SPI debe ser común a todos los miembros del grupo.
- Dirección IP destino.
- Identificador del protocolo de seguridad AH o ESP.
- La dirección destino que puede ser una dirección unicast o una dirección de grupo multicast.

La negociación de la SA y el SPI relacionado es parte integral del protocolo para el intercambio de llaves de seguridad.

Las asociaciones de seguridad forman una base de datos de seguridad SAD (Security Asociation Database).

Cuando un paquete IPv6 (igualmente con IPv4) es protegido con el protocolo IPSec, el encabezado de seguridad se inserta entre el encabezado principal y la carga útil, Fig. 3.4.5.8.2.3, si se usa el protocolo ESP para proteger los datos, además del encabezado IPSec después del encabezado principal, la carga útil es encriptada y se agrega un trailer ESP después de la carga útil encriptada.

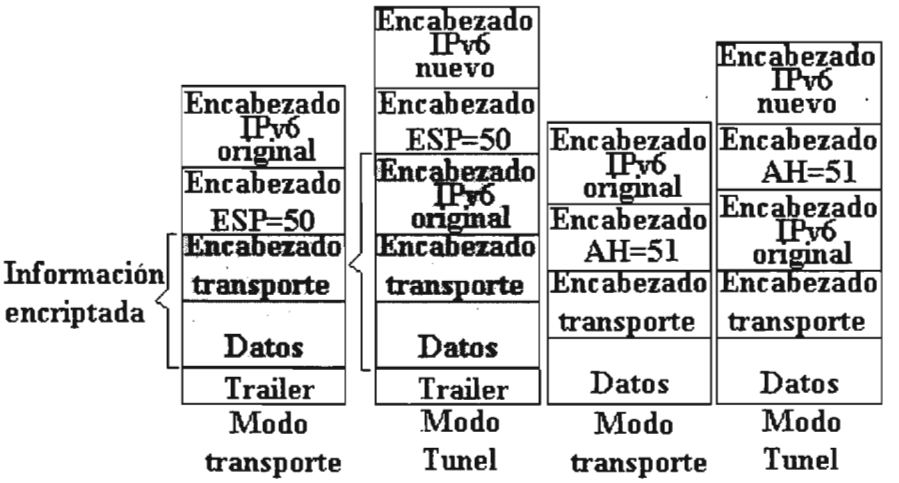


Fig. 3.4.5.8.2.3 Transmisión de los encabezados IPSec.

3.4.5.8.3 Administración de llaves

El sistema IPsec usa llaves para encriptar la información. La aplicación correcta de los encabezados AH y ESP requiere que las partes en comunicación acuerden una llave común a ser usada en la formación y comprobación de los encabezados de seguridad. Existen diferentes necesidades para el uso de estas llaves como son: intercambio de llaves rápido, autenticación fuerte, protocolos ligeros. IPv6 permite que la administración de llaves ocurra fuera de línea o mediante protocolos especialmente diseñados para ello.
La administración y distribución de estas llaves puede ser:

- Administración manual de llaves. Es una forma muy simple de administración de llaves de encriptación, consiste en que a cada sistema se le configura su propia llave y otras que necesite, debido a que esto es en forma manual y estática, solamente es aplicable prácticamente en ambientes pequeños. IPv6 requiere que cada implementación permita la configuración manual de las llaves de seguridad en caso de que no se tenga una técnica de administración en línea o se desee la seguridad basada en la intervención humana en ambientes restringidos con un numero pequeño de dispositivos seguros.
- Administración automática de llaves. Es una forma de creación de asociaciones de seguridad SA según se requieran, es decir por demanda. El método por default usado para implementar este sistema es el intercambio de llaves por Internet IKE (Internet Key Exchange) o IKMP (Internet Key Management Protocol) que funciona a nivel de aplicación y es independiente de los protocolos de capas inferiores.

El intercambio de llaves por Internet IKE es un método que dinámicamente autentica las puntas de la asociación IPSec, negocia los servicios de seguridad y genera las llaves compartidas. Para esto básicamente acopla el protocolo de administración de llaves y asociaciones de seguridad ISAKMP (Internet Security Association Key Management Protocol) y el protocolo de intercambio de llaves OAKLEY, los cuales definen procedimientos para autenticar la comunicación, la creación y administración de SA´s, técnicas de generación de llaves, etc. ISAKMP define una arquitectura genérica para el arreglo de SA autenticadas y el intercambio de llaves, puede ser usado con diferentes

técnicas de intercambio de llaves. OAKLEY es una versión modificada del algoritmo Diffie-Hellman.
Otra solución que se ha propuesto es SKIP (Simple Key Management for Internet Protocols) que basa su operación en el algoritmo Diffie-Hellman, este protocolo es simple maneja algunos problemas de administración de llaves en redes de alta velocidad, como el arreglo de llaves zero-messages y actualizaciones que permiten el rellaveo dinámico (cambios frecuentes en línea de las llaves de seguridad para evitar ataques analíticos basados en la acumulación de texto cifrado encriptado con la misma llave).
Los encabezados AH y ESP se pueden usar para proteger de diferentes formas las comunicaciones IP, como con el uso de redes privadas virtuales.
Los servicios de seguridad pueden ser ofrecidos para:

- Controlar el acceso.
- Checar la integridad de servicios no orientados a conexión.
- Verificar la confiabilidad de los datos mediante la autenticación del origen de los datos.
- Proteger al sistema contra replicas.
- Asegurar que la confidencialidad de los datos se ejecute mediante el encriptamiento de estos.

Redes privadas virtuales.
Las redes privadas virtuales VPNs (Virtual Private Network) proporcionan un camino seguro para la comunicación entre dos redes a través del uso de túneles.
El concepto de Tunneling (túnel) surge de la necesidad de transportar datagramas no ruteables por Internet dentro de datagramas IP. Se puede definir el tunneling como el transporte de un datagrama dentro de otro datagrama. El datagrama que se transporte dentro de otro datagrama puede ser IP, IPX, IPv6.
El túnel permitirá ocultar los datagramas dentro de otros datagramas para que sean transparentes las redes, dispositivos de comunicaciones y en general a la infraestructura de red.
En IPv4 las VPNs se construyen mediante la técnica de tunelización de IP donde los paquetes IP son protegidos y envueltos en una envoltura de seguridad y son encapsulados dentro de paquetes IP normales que solamente son usados para transportar los paquetes originales a través de la red publica a su destino final. Normalmente los extremos del túnel no son los hosts que desean intercambiar datos, mas bien son dos firewalls que protegen las LANs de ataques externos, como se muestra en la Fig. 3.4.5.8.3.1.

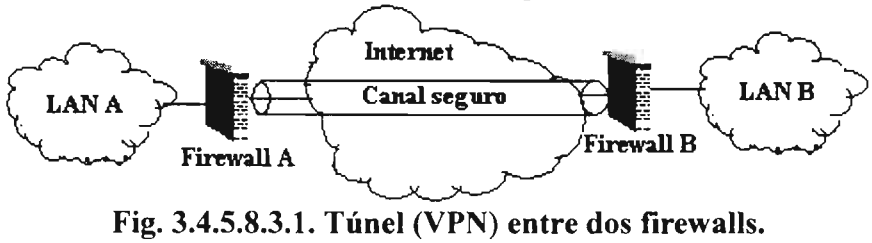


Fig. 3.4.5.8.3.1. Túnel (VPN) entre dos firewalls.

La creación de una VPN en IPv6 es más fácil y más estándar que en IPv4 en base a los encabezados AH y ESP. Así si quiere proteger contra manipulación y falsificación la comunicación entre dos hosts en las redes de la Fig. 3.4.6.10, se puede hacer uso del encabezado AH entre los firewalls, Fig. 3.4.5.8.3.2:

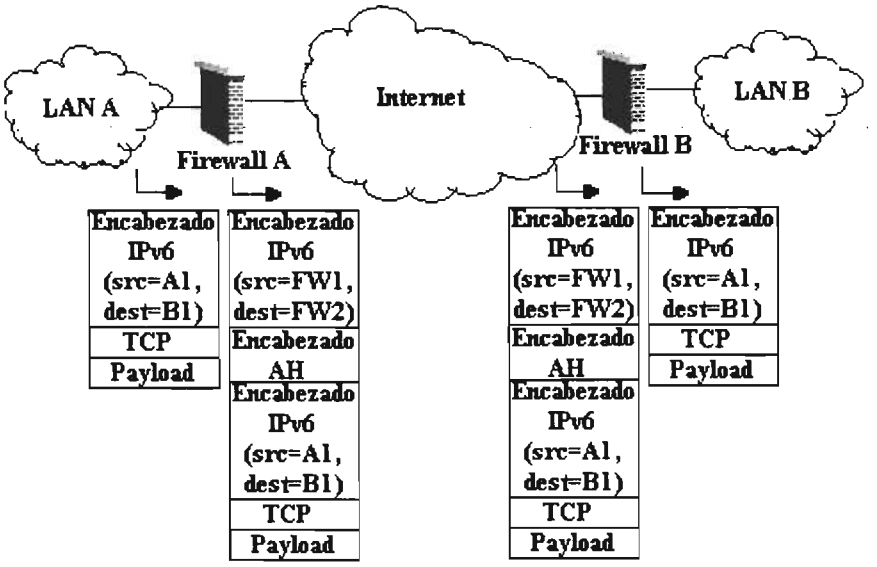


Fig. 3.4.5.8.3.2 Creación de una VPN en IPv6 mediante el encabezado AH.

Como se observa en la figura el FW A toma el paquete IPv6 y le agrega el encabezado AH antes de mandarlo al FW B. El FW B al recibir el paquete checa la integridad y autenticación de los datos usando los datos del encabezado AH., si todo es correcto remueve el encabezado AH y manda el resto al equipo B1. Se puede hacer uso de ESP para agregar encriptamiento al contenido de los datos.

Como se puede ver, comparando las dos formas de crear VPNs de IPv4 e IPv6 es la misma arquitectura pero debido a que IPv4 no permite el uso de múltiples encabezados el túnel tiene que ser implementado por alguna forma de encapsulación de IP en IP, lo que trace problemas de compatibilidad entre firewalls de diferentes fabricantes, se tendrá que realizar la fragmentación y reensamblaje en ambos extremos si al encapsular un paquete IP en otro paquete IP por rebasar el tamaño máximo permitido lo que degrada el desempeño del canal virtual.

En IPv6 la técnica VPN también puede ser implementada y un host, Fig. 3.4.5.8.3.3.

Fig. 3.4.5.8.3.3 Túnel (VPN) entre un firewall y un host.

Este caso se puede aplicar cuándo se tiene un host móvil que se conecta fuera del perímetro de red protegido, el FW funciona como home agent redireccionando los paquetes que van hacia la dirección externa del host móvil, después de agregar los encabezados AH o ESP respectivos.

3.4.5.9 Movilidad

Actualmente un numero creciente de usuarios no trabaja en sus escritorios de oficina, sino trabajan mientras viajan o se desplazan de un lugar dentro de su empresa. Así los empleados pueden querer trabajar en la misma forma en todos los lugares de trabajo conectando sus PCs portátiles a las redes de los diferentes lugares de trabajo o a las redes telefónicas. Asimismo los usuarios nómadas que viajan mucho y raramente están en sus oficinas pueden estar equipados con una PC móvil con una tarjeta PCMCIA para un teléfono móvil con la cual se conectan a Internet a través de una red móvil a través de radiofrecuencia requieren que les sea proporcionado el servicio de conectividad mediante la movilidad.
El tema de movilidad además de poder ser ofrecido debe tratar con una serie de problemas como la transmisión de radio (confiabilidad, roaming, hand-off), problemas de los protocolos IP (identificación, direccionamiento, configuración, ruteo) hasta los problemas de seguridad. IPv6 ofrece el servicio de movilidad, Fig. 3.4.5.9.1.

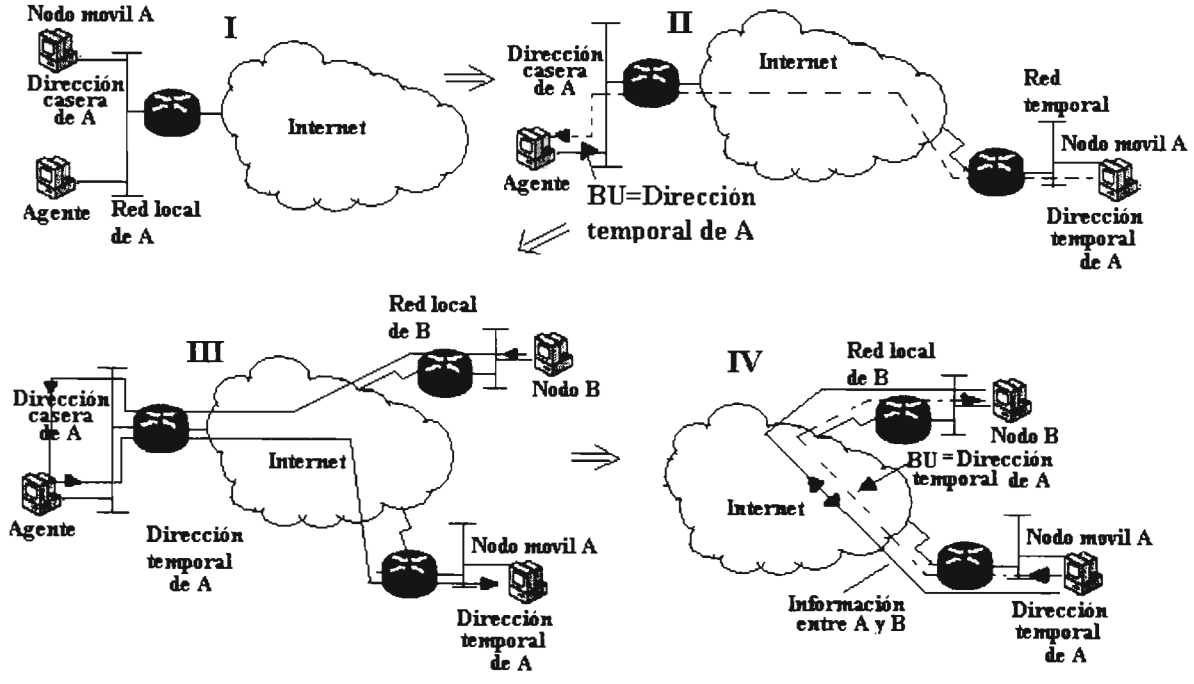


Fig. 3.4.5.9.1 Concepto de movilidad

Existen una serie de elementos o términos que intervienen en el esquema de movilidad IPv6 que son:

- Nodo móvil.
- Home address: Dirección local a la subred del nodo móvil.
- Care-of-address: Dirección temporal obtenida por el nodo en alguna red diferente a la suya.
- Home Subnet o Home Network: Red local del nodo movil.
- Foreign subnet o Foreign Network: Red exterior a la que se conecta un nodo móvil.
- Home agent. Router que mapea las relaciones entre direcciones locales y temporales.

- Binding Update: Mensajes de actualización de direcciones temporales.
- Cache Binding: Memoria que almacena los mapeos entre direcciones locales y temporales.

Operación del nodo móvil

Los problemas de administración de movilidad en IPv6 son problemas de administración de relaciones entre direcciones locales (home address) y direcciones temporales (care-of-address). El mapeo entre la dirección local y las direcciones temporales es conocido como binding.

Con la movilidad un nodo A que se conecte en diferentes partes podrá seguir recibiendo información de algún nodo B que requiera tener comunicación con él y su dirección local (home address). Cuando el nodo móvil A se percata de que se encuentra en una subred diferente (foreign subnet) a la suya (home subnet), obtiene una dirección temporal (care-of-address) de dicha red, mediante un proceso de autoconfiguración stateless o stateful en base a los mensaje de anunciamiento de router recibidos y a los bits M y O. Cada vez que el nodo móvil cambia de una subred IPv6 a otra subred IPv6 cambia su dirección temporal primaria, las anteriores son mantenidas para mantener terminar comunicaciones incompletas en esquemas de radio.

Cuando el host móvil se conecta a una red diferente debe delegar a un router (home agent) de su red local para que lo represente cuando esta ausente. Este home agent normalmente sirve a todos los nodos móviles de la red local reenviadoles los mensajes direccionados a ellos. Para ello el home agent traza todos los movimientos y registra en una memoria de enlaces (binding cache) los mapeos entre direcciones locales y temporales.

Para implementar este concepto se parte de que cada nodo móvil puede tener una o más direcciones y cuenta con una dirección que no cambia aunque el nodo se desplace, esto no quiere decir que el nodo viaja llevando consigo esa dirección, esta dirección conocida como dirección local (home address) será mantenida en la red local (home subnet) del nodo por medio de un agente local (home agent) el cual se encargara de redireccionar la información enviada por el nodo B dirigida al nodo A.

El agente (router en la red local) sabrá a donde redireccionar la información por que cuando el nodo móvil se mueve y se conecta en alguna otra red mediante una dirección temporal (care of address) informa esta dirección al agente (registra la dirección temporal en el agente) por medio de un mensaje BU (Binding Update) y la almacena en su binding cache. para que cuando el agente reciba información en la dirección casera de A le reenvíe esta información a su dirección temporal. El mensaje BU también debe ser mandado a todos los hosts con los cuales el nodo móvil tuvo intercambio de paquetes, los cuales podrían tener información incompleta en su binding cache. Por esto el nodo móvil debe tener una lista conocida como Binding Update List que contiene las direcciones de todos los nodos a los cuales les mando mensajes BU y su restante validez temporal. El mensaje BU debe incluir un encabezado de autenticación para evitar situaciones de hackeo como redireccionamientos o uso fraudulento.

Un nodo móvil puede ser alcanzado en cualquier momento, mandando un mensaje a su dirección local. El agente intercepta la información enviada a la dirección local del nodo móvil y la reenvía a la dirección temporal primaria a través de un túnel mediante un proceso de encapsulación y el uso de IPSec para proteger la señalización entre el nodo móvil y el agente local.

Una vez que el nodo A recibe la notificación de información redirigida a el proveniente del nodo B a través del agente, el nodo A se comunicara directamente con el nodo B a través de mensajes BU para informarle su ubicación mediante su dirección temporal. Cuando el nodo fuente del mensaje B recibe el mensaje BU crea en su cache binding una entrada que contiene la dirección local y temporal del nodo A. Esta información permite al nodo B directamente enviar los siguientes paquetes a la dirección temporal de A, a través de un encabezado de ruteo, en lugar de a través de un túnel (usado por el agente). Por lo tanto solamente el primer paquete intercambiado entre un nodo fuente B y el nodo móvil A pasara a través del agente. Los posteriores intercambios de información se realizaran directamente entre los nodos A y B sin la intervención del agente y a través del encabezado de ruteo..
IPv6 proporciona el soporte de la movilidad a nivel macro es decir para moverse de una red Ethernet a otra, o de una red Ethernet a una inalámbrica, pero para la movilidad micro (movimiento entre celdas de una red inalámbrica) no es muy apropiado.

Opciones para el manejo de movilidad
La información necesaria para soportar la movilidad de un host IPv6 es intercambiada a través de cuatro opciones implementadas en un encabezado de extensión Opciones Destino. Las opciones pueden estar asociadas con:

- Paquetes IPv6 normales que contienen payloads como TCP o UDP.
- Paquetes independientes que contienen solamente opciones. Aquí el campo next header debe ser igual a 59.

Las opciones son codificadas en un formato TLV (Type, Length, Value).

- **Opción Binding Update**

Un nodo móvil usa la opción Binding Update (BU) para comunicar a su home agent o nodos correspondientes su actual mapeo (binding). El formato de esta opción se muestra en la Fig. 3.4.5.9.2.

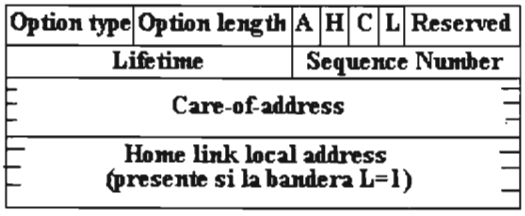


Fig. 3.4.5.9.2 Opción Binding Update

Los campos de la opción BU son:

- Option type: Campo de 8 bits con valor 192. Sus tres bits tienen un significado especial, debido a que el campo vale 192, dichos tres bits valen 110 que indican:
  - Para el caso de los dos primeros bits (11), si un nodo no reconoce la opción, debe descartar el paquete y comunicar esto al nodo fuente a través de un mensaje ICMPv6 problema de parámetros, solo si la dirección destino no es multicast.
  - El tercer bit (0) indica que la opción no puede ser modificada en la ruta.
- Option Length: Campo de 8 bits que contiene la longitud en octetos de la opción sin incluir los campos Option type y Option length. Su valor mínimo es 6 si las direcciones temporal (care-of-address C=0) y de enlace local (home link local

address L=0) no están presentes. Su valor máximo es 38 si están presentes (C=1, L=1).

- El campo de 1 bit A (Acknowledge) es puesto por el nodo fuente para solicitar al nodo que recibe la opción BU que mande un mensaje de reconocimiento de mapeo BA (Binding Acknowledgment)
- El campo de 1 bit H (Home registration) es puesto por el nodo fuente para solicitar al nodo que recibe la opción BU que funcione como su home agent. La dirección destino del paquete IPv6 que contenga esta opción debe ser la de la interfaz de un router cuyo prefijo es igual a la dirección local (home address) del nodo móvil.
- El campo de 1 bit C (Care-of-address presente) es puesto por el nodo fuente para indicar la presencia de la dirección temporal en la opción BU.
- El campo de un bit L (Dirección de enlace local presente) es puesto por el nodo fuente para indicar la presencia de la dirección de enlace local en la opción BU. Este bit es puesto por el nodo fuente para solicitar al nodo destino funcionar como un proxy, esto es, que participe en el proceso de descubrimiento de vecinos ND en lugar del nodo móvil. Si este bit es establecido el bit H tambien debe ser establecido.
- Reserved: Campo de 12 bits reservado para uso futuro, debe valer cero para la transmisión e ignorado por la recepción.
- Lifetime: Campo de 16 bits que contiene el intervalo valido de información de mapeo (binding) en segundos en la memoria de mapeo (cache binding). Un valor cero indica que la información de mapeo debe ser borrada de la memoria de mapeo, un valor 0xFFFF indica que la información de mapeo debe ser mantenida indefinidamente.
- Sequence number: Campo de 16 bits usados para el mapeo entre mensajes BU y BA. Cada BU mandado por un nodo móvil debe usar un numero de secuencia mayor que el numero de secuencia del BU previo a la misma dirección destino.
- Care-of-address: Campo de 128 bits que contiene la dirección temporal IPv6 adquirida por el nodo móvil en una red externa (foreign network). Cuando la dirección temporal es puesta igual a la dirección local, indica que es necesario cancelar las asociaciones de memoria de mapeo para el nodo móvil y que no se debe crear una nueva asociación.
- Home link local address: Campo de 128 bits que contiene la dirección de enlace local IPv6 usada por el nodo móvil durante su ultima conexión en la red local. Este campo es opcional y se presenta si el campo L=1.

- **Opción Binding Acknowledgment**

Esta opción confirma la recepción de la opción BU, solamente si el nodo móvil lo solicita con la bandera A, su formato se muestra en la Fig. 3.4.5.9.3.

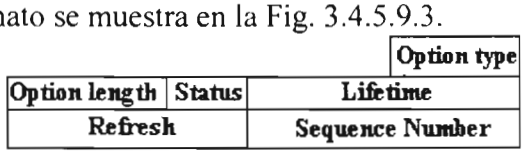


Fig. 3.4.5.9.3 Opción Binding Acknowledgment

Los campos de esta opción son:

- Option type: Campo de 8 bits con valor 193.

- Option Length: Campo de 8 bits que contiene la longitud en octetos de la opción sin incluir los campos Option type y Option length. Su valor es 9.
- Status: Campo de 8 bits que usa los valores de la siguiente tabla:

Valor	Significado
0	Opción aceptada
128	Opción rechazada: razón no especificada
129	Opción rechazada: BU pobremente formado
130	Opción rechazada: operación prohibida administrativamente
131	Opción rechazada: insuficientes recursos
132	Opción rechazada: registro local no soportado
133	Opción rechazada: la red no es la red local
134	Opción rechazada: Valor del campo numero de secuencia muy pequeño
135	Opción rechazada: respuesta al descubrimiento de la dirección del home agent dinámica.

Los valores menores a 128 indican que la opción BU ha sido aceptada, valores mayores o iguales a 128 indican que ha sido rechazada.

- Lifetime: Contiene el tiempo que el nodo mantiene la información almacenada en su memoria de mapeo (binding cache).
- Refresh: Es el periodo de tiempo después del cual el nodo móvil debe mandar un mensaje BU para actualizar la información de su memoria de mapeo.
- Sequence number: Campo de 16 bits usados para el mapeo entre mensajes BU y BA.

Los campos opcionales que no se han definido todavía se pueden agregar después de la opción binding acknowledgment.

- **Opción Binding Request.**

Esta opción se usa para solicitar al nodo móvil que mande un mensaje BU. Es usada por un nodo con una entrada en la memoria de mapeo cuya validez temporal esta por expirar, de esta manera se obtiene la información actualizada. El formato de esta opción es el de la Fig. 3.4.5.9.4.

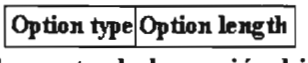


Fig. 3.4.5.9.4 Formato de la opción binding request.

Los campos de esta opción son:

- Option type: Campo de 8 bits con valor 194.
- Option length: Campo de 8 bits que contiene la longitud en octetos de la opción sin incluir los campos Option type y Option length. Su valor es 0.

Los campos opcionales que no se han definido todavía se pueden agregar después de la opción binding request.

- **Opción Home Address.**

Esta opción se incluye en un paquete mandado por un nodo móvil para informar al destino del paquete de la dirección local (home address) del nodo móvil. El formato de esta opción es el de la Fig. 3.4.5.9.5.

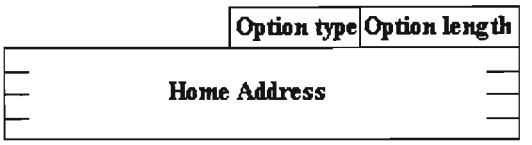


Fig. 3.4.5.9.5 Formato de la opción home address.

Los campos de la opción home addres son:

- Option type: Campo de 8 bits con valor 195.
- Option Length: Campo de 8 bits que contiene la longitud en octetos de la opción sin incluir los campos Option type y Option length. Su valor es 8.
- Home address: Campo de 128 bits que contiene la dirección local (home address) IPv6 del nodo móvil que transmite el paquete.

Los campos opcionales que no se han definido todavía se pueden agregar después de la opción home address.

Requisitos generales a ser cumplidos por todos los nodos IPv6 de una arquitectura de movilidad

Todos los nodos IPv6 deben cumplir los siguientes requisitos:

- Recibir una opción BU y generar un mensaje de reconocimiento de mapeo BA (binding acknowledgment).
- Administrar una memoria de mapeo BC (binding cache) para almacenar la información recibida por los mensajes BU.
- Administrar una asociación de seguridad para ser usada conjuntamente con el encabezado de autenticación IPv6, para poder almacenar en su BC la información de un mensaje BU se debe checar la identidad del nodo fuente.

Requisitos a ser cumplidos por los routers de una arquitectura de movilidad

Los routers IPv6 pueden contener información de un nodo móvil en su BC, por lo que deben cumplir los siguientes requisitos:

- Cada router IPv6 debe ser capaz de usar su BC para rutear paquetes. Así si un router tiene en su BC una entrada para la dirección destino, debe encapsular el paquete en un túnel y mandarlo a la dirección temporal.

Además de permitir a un nodo dejar su red local, por lo menos un router en la red local debe ser capaz de operar como un agente local (home agent), el router que opere como agente debe cumplir los siguientes requisitos adicionales a los de los routers:

- Administrar una lista de nodos para los cuales ellos operan como agentes.
- Interceptar los paquetes dirigidos a nodos móviles sobre la red local, reemplazando a los nodos móviles en el procedimiento neighbor discovery.
- Retransmitir los paquetes interceptados creando un túnel hacia las direcciones temporales de los nodos móviles.

Requisitos a ser cumplidos por los nodos móviles de una arquitectura de movilidad

Los requisitos que deben cumplir los nodos móviles son:

- Recibir paquetes a través de un túnel.
- Mandar mensajes BU y recibir mensajes BA.

- Administrar una lista de mensajes BU en la que almacenen todos los nodos que han mandado mensajes BU cuya validez temporal no ha expirado.
- Detección de la movilidad
  Un nodo móvil debe usar todos los mecanismos a su disposición para detectar la movilidad. El principal es el descubrimiento de vecinos ND. El procedimiento ND localiza la presencia de nuevos routers y nuevos prefijos de red. También debe usar el procedimiento de detección de inalcanzabilidad de vecinos para comprobar la alcanzabilidad de su router por default.
- Detección del regreso a su red local.

El nodo móvil detecta que esta de vuelta en su red local, cuando recibe los prefijos de su red local a través de mensajes ND, por lo que el nodo móvil transmite a su agente local un mensaje BU en el que la dirección temporal es igual a su dirección local, de esta manera solicita al agente que ya no intercepte los paquetes dirigidos a el. El mensaje BU debe ser transmitido con el bit A=1 y repetido hasta que el agente local mande un mensaje BA.
También el nodo móvil debe mandar un mensaje de anunciamiento de vecino con la bandera override puesta, para solicitar a los hosts en la red local que actualizasen su información de vecinos en sus memorias, esta operación se debe realizar tanto para las direcciones local y de enlace local.

3.4.5.10 Aplicaciones

El nuevo direccionamiento esta pensado para cubrir necesidades de aplicaciones con gran capacidad de direccionamiento, debido a que en el futuro los dispositivos electrodomésticos, electrodomésticos y dispositivos eléctricos en general serán computadoras como es el caso de la conectividad para vehículos móviles como automóviles, teléfonos celulares con terminales Java para navegar en Internet. Actualmente existen sistemas de iluminación domésticos en los que las lámparas tienen una dirección y son apagadas y encendidas por mensajes mandados por switches. En el futuro los usuarios de Internet pueden querer ordenar desde fuera de sus casas que un horno comience a cocinar un pavo, o pueden querer recibir un mensaje desde la alarma de su casa que les informe de posibles intromisiones, acceso a Internet desde televisores, automatización o manejo de aparatos domésticos desde Internet como puede ser el surtido de un refrigerador si este se ha quedado sin alimentos, el encendido de una lavadora desde el trabajo a través de Internet, etc.
IPv6 esta diseñado para cumplir los requerimientos de aplicaciones como asistentes personales digitales habilitados para Internet (PDAs), redes de área casera (HAN), transportaciones conectadas por Internet (por ejemplo automóviles), la capacidad de proporcionar una dirección única para cada dispositivo de red habilita el alcance de extremo a extremo lo cual es especialmente importante para proporcionar servicios de telefonía IP integrada residencial, servicios inalámbricos IP y juegos distribuidos. IPv6 además de cumplir con estos requerimientos permite regresar a un ambiente global donde las reglas de direccionamiento de la red son otra vez transparentes a las aplicaciones.
Los principales promotores de IPv6 que impulsaron sus características y están provocando cada vez más aplicaciones de IPv6 son los usuarios y proveedores de servicios always-on como:

- Servicios y redes inalámbricas, IPv6 móvil y de tercera generación. IP móvil es una de las aplicaciones que más ha impulsado a IPv6 ya que existen mas de 2 billones de dispositivos móviles (vehículos, teléfonos celulares) que están habilitados para conectarse a Internet a los cuales solo IPv6 ofrece suficientes direcciones y la conectividad móvil necesaria.
- ADSLv6
- Redes caseras, juegos en línea, etc.

Otras aplicaciones que requieren direcciones IP de ámbito global, únicas y ruteables son:

- Voz sobre IP VoIP.
- Videoconferencia.
- Juegos.
- IPSec.

Las aplicaciones básicas y genéricas existentes en IPv4 utilizadas generalmente como utilerías o herramientas para probar la conectividad entre hosts ha sido actualizadas para funcionar con IPv6, herramientas como son:

- Ping6. Esta aplicación es una herramienta idéntica ala utilería Ping usada en IPv4 para probar la alcanzabilidad de algún host en la red y conocer el tiempo que tarda en contestar una solicitud para determinar la lejanía de dicho equipo, Ping6 esta habilitada para funcionar con direcciones IPv6, es decir con 128 bits.
- Tracerouter6. Esta aplicación es la versión actualizada de traceroute de IPv4, con esta utilidad se obtiene un registro de la ruta que sigue un mensaje a través de Internet hasta el host destino informando del tiempo total de cada salto, con esta misma utilería se obtiene un detalle de los equipos que componen la ruta desde la fuente al destino y nos ayuda a determinar en que punto de la red se encuentra algún problema. Tracroute6 o tracepath6 también ya maneja direcciones IPv6.
- Ttcp esta aplicación básica usada para checar el tiempo de transmisión y recepción de datos TCP y UDP entre dos equipos funciona tanto para IPv4 como para IPv6.

Actualmente en eventos como el lanzamiento del servicio global de IPv6 se han empezado a presentar y observar aplicaciones reales de IPv6 como:

- Uso de IPv6 en el espacio para la comunicación vía satélite mediante tecnologías como DVB-S/MPEG-2.
- Televisión de alta definición con IPv6 y calidad de servicio HDTV/IPv6 y QoS.
- Videoconferencias multicast con IPv6 mediante la red M6Bone.
- IPv6 en el hogar para el control remoto de electrodomésticos, cortinas, vigilancia mediante cámaras, etc.
- IPv6 en ambientes de colaboración a distancia.
- Aplicaciones de videoconferencia y voz sobre IP (VoIP) con IPv6.
- El canal de televisión digital Euronews.
- Uso de IPv6 en video digital y en el control remoto de instrumentos como microscopios, telescopios, etc.
- Demostraciones de IPsec con IPv6.
- Uso de IPv6 en un automóvil usando tecnologías como GPRS, Bluetooth y WiFi para redes inalámbricas.
- Herramientas de administración y monitoreo con soporte IPv6.
- Transmisión de IPv6 sobre enlaces PLC, etc.

Implementaciones de plataformas con IPv6

IPv6 ya es soportado en la mayoría de los sistemas operativos Algunas implementaciones de sistemas comerciales en software a nivel de host con IPv6 son:

- Apple computer tiene un prototipo de implementación de IPv6 funcionando en un sistema abierto de Apple. El sistema operativo con soporte IPv6 es la versión 10.2 Jaguar que viene con MAC OS X.
- Hewlet Packard ha implementado IPv6 con el sistema operativo HP-UX 11.0.
- BSD. BSD fue uno de los primeros sistemas operativos en soportar IPv6 por lo que actualmente es el mas actualizado, esto es debido a que este fue el sistema operativo en el que los desarrolladores del proyecto KAME realizaron las implementaciones de las más nuevas características de IPv6. Así existen algunas variantes de BSD como
  - OpenBSD. Este es un sistema operativo que maneja IPv6 desde la versión 2.7. Porta aplicaciones IPv6.
  - NetBSD. Como el OpenBSD también contiene la pila KAME. Porta aplicaciones IPv6.
  - FreeBSD. Tambien incluye la pila KAME. Porta aplicaciones IPv6.
- BSDI participa en el proyecto 6BONE con la implementación de IPv6.
- Digital ha implementado un prototipo de IPv6 en su Alpha Unix y Alpha Digital Open VMS.
- IBM tiene múltiples implementaciones en hosts en maquinas de RS6000 y S/390 y soporta completamente IPv6 en AIX.
- Novell desarrolla una implementación completa de IPv6 que incluye autoconfiguración, movilidad, seguridad, OSPF, DHCP, PPP e integración IPX.
- Siemens esta desarrollando una implementación completa para Iris y en sus sistemas operativos BS2000/OSD.
- Silicon graphics con el sistema operativo Irix.
- Sun microsystems desarrolla la implementación de IPv6, los sistemas Solaris 8 y 9 soportan completamente IPv6 corriendo en procesadores SPARC y maquinas x86.
- Microsoft con Windows NT, 2000, XP y 2003 Server. Microsoft ha puesto interés en IPv6 y desarrolla su propia pila IPv6. Tal pila IPv6 esta incluida únicamente en Windows XP y posteriores como Windows Server 2003. La capacidad de IPv6 de Microsoft incluye el Internet Explorer y aplicaciones como ping, traceroute, o tracepath. Para Windows 2000 con SP1 y superior se tiene disponible una tecnología previa de IPv6, la cual proporciona funcionalidad IPv6 basica para propósitos de prueba, no se tiene pensado desarrollar versiones de producción. Para Windows 95/98/NT Trumpet ha implementado una versión Winsock de IPv6.
- Compaq/Digital inicialmente implemento IPv6 en sus sistemas operativos Alpha Tru64 UNIX y Alpha Open VMS, ahora que pertenecen a HP se continua el trabajo sobre IPv6. Desde el 2001 HP/Compaq/DEC también ofrecen IPv6 con su sistema operativo OpenVMS (Alpha/IA64).
- Nokia con el sistema operativo EPOC-ER3 y ER5.
- Kame con Free, Open y NetBSD, BSDI BSD/OS.
- FreeBSD con el sistema operativo KAME.
- LINUX en sistemas operativos como Redhat, Debian y SUSE. El kernel de Linux es también una de las aplicaciones para IPv6 casi tan buenas como BSD debido a que

es usado en el proyecto USAGI así como BSD en KAME. Algunas variantes de Linux son:

- Debian fue una de las primeras distribuciones que incluyo IPv6.
- Red hat.
- SUSE.

Además de sistemas operativos y aplicaciones básicas que ya manejan IPv6, se están desarrollando un gran numero de aplicaciones comerciales para soportar IPv6.
En el área de software una gran cantidad de software de aplicaciones comerciales esta siendo actualizado para el uso, manejo y soporte de IPv6 como navegadores Web, servicios DNS, servidores http, juegos por Internet, servidores y clientes FTP, servidores y clientes Telnet, servidores y clientes de correo, software para conversación en línea, la tabla 3.4.5.10.1 muestra algunos ejemplos de software de aplicación que esta siendo o ya ha sido actualizado a IPv6:

Aplicación Comercial	Sistema operativo o plataforma	Función
Telnet		
Telnet	Windows	Servidor y cliente telnet
Telnet	BSD y LINUX	Servidor y cliente telnet
FTP		
Libra FTP daemon	LINUX	Servidor FTP anónimo. Soporta direcciones IPv4 e IPv6.
FTP	Windows	Cliente FTP
LFTP 2.0.x	LINUX GNU	Cliente ftp avanzado que soporta IPv6, disponible en http://ftp.yars.free.net/projects/lftp/
NcFTP	Windows, LINUX, BSD	Cliente FTP con soporte de IPv6 del proyecto KAME disponible en ftp://ftp.kame.net/pub/kame/misc, versión para Windows NT disponible en http://www.research.microsoft.com/msripv6
SSH		Parches para agregar capacidad IPv6 a SSH versión 1 del proyecto WIDE disponibles en ftp://ftp.kyoto.wide.ad.jp/IPv6/ssh/
DNS y proxies		
DNS	Windows	Servidor DNS
TotD	BSD	Proxy y DNS para traducir entre registros IPv4 e IPv6 para el soporte del NAT-PT
BIND 9	BSD, LINUX, UNIX	Servidor DNS
wwwoffle		Proxy WWW habilitado para IPv6 esta disponible en http://www.vermicelli.pasta.cs.uit.no/ipv6/software.html
Squid		Parches para agregar soporte para IPv6 al sistema cache web squid del proyecto KAME disponibles en

		ftp://ftp.kame.net/pub/kame/misc/
Cliente www		
Internet Explorer 5.5	Windows	Web browser. La actualización binaria para agregar capacidad IPv6 al Internet Explorer 4 esta disponible en http://www.research.microsoft.com/msripv6
Mozilla	BSD, LINUX, UNIX	Web browser soporta IPv6 nativamente desde el 2000 para su actualización http://www.mozilla.org/status/2000-04-11.html
Lynx 2.8.2		Lynx con soporte de IPv6 esta disponible en ftp://ftp.pasta.cs.uit.no/pub/Vermicelli/lynx-282-v6-19990829
Wget	Windows, UNIX	Web browser
W3m		Navegador www que accesa sitios IPv6 nativamente por lo que no necesita parches.
wMosaic		Mosaic multicast, es una implementación IPV6/IPv4 para http y FTP.
Servidor www		
Apache y Mini_hhtpd	BSD, linux	Servidor web. Parches para agregar capacidades IPv6 a Apache del proyecto KAME disponible en ftp://ftp.kame.net/pub/kame/misc/, http://ftp2.v6.linux.or.jp/pub/Linux/IPv6-2/apache/apache_1.3.11-v6-20000125.diff.gz
Mini_httpd	BSD, LINUX	Servidor web habilitado para IPv6 y SSH.
Fnord	Windows	Servidor web con capacidad IPv6, disponible en http://www.research.microsoft.com/msripv6
Thttpd		Servidor web seguro, rápido portátil, pequeño y simple, soporta IPv6 originalmente por lo que no requiere parches.
Servidor de correo		
Public sendmail	Windows	Servidor de correo
Wide sendmail	BSD	Servidor de correo
Sendmail 8.9.1	Parches para agregar soporte IPv6	Disponibles en ftp://ftp.kyoto.wide.ad.jp/IPv6/mail/
Fetchmail	BSD, LINUX, UNIX	Servidor de correo
Qmail	Parches para agregar soporte IPv6	disponibles en http://www.rcac.tdi.co.jp/fujiwara/
Exim		MTA seguro y confiable que soporta nativamente IPv6
Inframail		Puerto IPv6 que soporta SMTP y POP3.
Postie		Puerto IPv6 tiene SMTP, POP3, IMAP, etc

Analizador de protocolos		
Netmonitor	Windows	Analizador de protocolos
COLD	LINUX	Analizador de protocolos red y sniffer, es de distribución libre y el paquete esta disponible
Ethereal	Windows	Sniffer que soporta IPv6.
Multimedia		
RAT	Windows, LINUX	Software para chat. Versión habilitada con IPv6 de la herramienta de audio robusta RAT
SDR	Windows, LINUX	Software para chat. Versión del Directorio de sesión multicast habilitada con IPv6
IRC BitchX cliente	LINUX, UNIX, windows	Software para chat
Cyclone 1.0	BSD, LINUX	Software para chat
INN v.2.2.2	BSD, LINUX	Servidor de noticias
Quake		Juego multiusuario Quake IPv6 en http://www.viagenie.qc.ca/en/quake.shtml
VideoLAN		Servidor y cliente VideoLAN. El proyecto de contenido videolan sobre UDP o http usando IPv4 o IPv6
Mnews	BSD, LINUX	Cliente de noticias
MIPL	LINUX	Implementación para movilidad IPv6
Ipfilter	BSD, UNIX, Solaris, SunOS. HPUX	Firewall
IPFW	BSD	Firewall
netfilter	Linux	Firewall
Quakeforge	Windows, Linux, Unix, BSD	Juego en línea
Java IPv6	Windows	Java para windows
Exim	UNIX	Agente de transferencia de mensajes
Gmail	BSD	Agente de transferencia de mensajes
Toolnet6	Windows	Software para conmutación de protocolo para Windows 95/98 o Windows NT. Las aplicaciones que trabajen en estos sistemas pueden acceder por medio de este software tanto a redes IPv4 e IPv6
v6tun	BSD	Programa que permite hacer túneles IPv6 sobre IPv4. El túnel puede ser asegurado con SSH

Tabla 3.4.5.10.1 Algunas aplicaciones con soporte de IPv6

Algunas implementaciones de sistemas comerciales en ruteadores con IPv6 se listan en la tabla 3.4.5.10.2:

Fabricante	Comentario
3Com	Ha empezado a entregar funcionalidad IPv6 en sus productos y plataformas NetBuilder II y PathBuilder S500
Nortel Networks	Ha empezado a usar IPv6 a partir de la versión de software 12.0 de su suite de protocolos BayRS. Actualmente tiene soporte de IPv6 en hardware en su dispositivo de ruteo RSP2
Hitachi	Ha desarrollado sus ruteadores NR60 con IPv6 y la familia de routers gigabit GR 2000 capaces de reenviar trafico IPv6 por hardware
IBM	Soporta todos los beneficios de IPv6 en sus ruteadores
Sumitomo	Ha implementado ruteadores de la familia 3700 Suminet con IPv6
Cisco	A partir de la versión 12.2 soporta IPv6 en sus ruteadores, la 12.3 ya es una versión de producción.
Nokia	Maneja IPv6 con el sistema operativo IPSO 3.3. Nokia es un desarrollador e investigador muy activo de IPv6 principalmente en el area móvil y de 3ª generación.
Juniper networks	Todos los routers de Juniper contienen funcionalidad IPv6 desde el release 5.1 del sistema operativo JunOS. Desde el reléase 5.2.de JunOS también incluye características de administración IPv6 como transporte IPv6 para SNMP.
Fujitsu	Con la serie Geostream R900 proporciona soporte completo para IPv6 y retransmite trafico IPv6 por hardware
Extreme Networks	Tiene su versión habilitada para IPv6 ExtremeWare 7.0 para switches de capa 3 de la serie BlackDiamond (6808 y 6804), Alpine (3808 y 3804) así como la serie Summit i. También ha desarrollado un modulo MPLS en el BlackDiamond que reenvía trafico IPv6 por hardware.
Zebra	Es un paquete de software para ruteo que funciona en sistemas operativos UNIX y BSD, soporta IPv6.
Proyecto Merit	Desarrolla software para ruteo, análisis y administración de red para diferentes plataformas y protocolos, desde el año 2000 libero sus primeros códigos binarios para soportar IPv6 en Windows 2000 y XP

Tabla 3.4.5.10.2 Ruteadores con soporte de IPv6.

En la tabla 3.4.5.10.3 tenemos una lista de algunos routers relay públicos, que se encuentran disponibles para realizar pruebas con IPv6.

Nombre	Contacto	Nota
Global		
2002:c058:6301::	No hay	Esta es una dirección anycast para el router relay más cercano
Norteamerica		
6to4.ipv6.Microsoft.com	Microsoft	Abierto-disponible
ipv6-lab-gw.cisco.com	Cisco	Uso por petición en la pagina IPv6 de Cisco
Océano pacifico /Asia		
6to4.ipv6.aarnet.net.au	AARNET NOC	Abierto solamente a Australia o las proximidades
kddilab.6to4.jp	Kddilab	Abierto-disponible
6to4.ipv6.ascc.net	Academia sinica de computación	Abierto experimental
Africa		
6to4.ipng.unix.za.net	Univ. de Capetown	Abierto-disponible
Europa		
6to4.ipv6.bt.com	Stuart Prevost	Abierto-disponible
skbys-00-00.6to4.xs26.net	Acess to six	Abierto-disponible
6to4.ipv6.uni-leipzig.de	uwe	Abierto experimental
6to4.ipv6.fh-regensburg.de	Hubert Feyrer	Abierto experimental
6to4.ipng.nl	Pim Van Pelt	Abierto-disponible

Tabla 3.4.5.10.3 Lista de routers relay disponibles en Internet para pruebas.

Podemos ver con estos ejemplos listados que ya existe una incontable numero de marcas tanto de sistemas operativos, aplicaciones y ruteadores que ya soportan IPv6, gracias a todo este software y hardware que manejan IPv6 la migración sera más fácil y el tiempo de su ejecución será menor. Realmente el punto faltante es usar estas aplicaciones, sistemas operativos o ruteadores que ya existen, funcionan y se encuentran disponibles para empezar a manejar IPv6, con lo cual la transición a IPv6 pueda ser realizada en menos tiempo.

3.4.6 Autoconfiguración de Direcciones

Por la definición propia de autoconfiguración una computadora debería automáticamente descubrir y configurar los parámetros necesarios para conectarse a Internet. La autoconfiguración de direcciones es una de las principales características que ofrece el protocolo IPv6, esta autoconfiguración no tiene que ser necesariamente aplicada a maquinas móviles ya que de hecho se aplica a cualquier nodo, sea móvil o no.
Los datos de las redes son cada vez más complejos y la necesidad de eliminar algunas dificultades hace al Plug and Play imprescindible. El usuario no tiene que conocer en detalle la arquitectura de la red, ni saber configurar el software de red de su estación de trabajo. Prácticamente el usuario solo debería saber conectar su equipo a la red y verlo

funcionar sin necesidad de introducir funciones de especialista. Puede haber preocupaciones de seguridad para limitar este nivel de transparencia de auto configuración de direcciones en algunos entornos pero los mecanismos deben existir para soportar cualquier automatización.
El proceso de autoconfiguración IPv6 incluye la creación de una dirección de enlace local y la verificación de que es única sobre el enlace, al mismo tiempo se debe determinar que información debe ser autoconfigurada y en el caso de direcciones se debe determinar si estas deben ser obtenidas a través de un mecanismo stateless, un mecanismo stateful o la combinación de ambos.
IPv6 define dos mecanismos de autoconfiguración de direcciones:

- El mecanismo de autoconfiguración de dirección stateless.
- El mecanismo de autoconfiguración de dirección stateful.

3.4.6.1 Autoconfiguración stateless

La configuración stateless o serverless es parte integral de IPv6 y se realiza sin ninguna configuración manual, mínima configuración de los routers y no requiere el uso de servidores, esta configuración es realizada automáticamente por los equipos por lo que es conocida también como plug and play (conectar y usar).
La primera exigencia de la operación Plug and Play es que una estación pueda ser capaz de adquirir una dirección de manera dinámica ya sea cuando es conectada por primera vez a una red o cuando la estación necesite ser reconfigurada por traslado o por que la identidad de la red ha sido modificada. Existen otras funciones Plug and Play que la mayoría se hace fuera del protocolo IPv6, pero el protocolo de autoconfiguración de direcciones de una estación será ejecutado por IPv6.
Este tipo de configuración cumple los siguientes requerimientos:

- Antes de conectarse un host IPv6 a la red ninguna forma de configuración manual se requiere. Un mecanismo debe crear automáticamente una dirección única por cada interfaz.
- Los hosts de redes pequeñas no deben requerir la presencia de un servidor stateful DHCP o de un router para comunicarse por medio de direcciones de enlace local autoconfiguradas.
- Los hosts y routers de grandes redes no deben requerir la presencia de servidores stateful DHCP por medio de direcciones globales o de site local derivadas de la lista de prefijos asociadas con enlaces proporcionadas por los anunciamientos de router.
- Debe simplificar las operaciones de renumeración (cambio de direcciones)
- Se debe permitir al administrador especificar si usan autoconfiguración stateless o stateful o ambos.

La configuración stateless puede usarse en:

- Ambientes donde no existen equipos de ruteo.
- Ambientes donde si existen los ruteadores.

- **Autoconfiguración stateless en ambientes donde no existen equipos de ruteo.**

Cuando la configuración stateless se usa en un ambiente sin anunciamiento de ruteadores, los equipos autoconfiguran direcciones del tipo link local o intraenlace, estas direcciones son usadas para tener conectividad local al segmento ethernet.

Cuando un nodo no recibe un prefijo por anunciamiento de router por default asignara como prefijo de la dirección el de link local FE80, ya que como lo importante al inicio de que un nodo es conectado a una red es tener conectividad local a la red a la que se encuentra conectado, por ello se usa este prefijo para poderse comunicar con los hosts u otros nodos que se encuentren conectados a la misma red local por medio de mensajes de solicitud de vecinos usando multicasting.
La autoconfiguración de direcciones también puede ser usada en maquinas móviles (plug and play) a las cuales se les asigna automáticamente una dirección IP cada vez que se conecten a una red. En IPv6 cualquier nodo auto configurará sus direcciones IPv6, por lo que un nodo autoconfigura una dirección de tipo link local inicialmente cuando es conectado a la red, no importando si se le ha configurado una dirección IPv4 o no.
El nodo automáticamente genera las direcciones basándose en su dirección MAC para generar el identificador de interfaz en formato EUI-64. Para acabar de construir la dirección IPv6 el nodo antepondrá al numero resultante del proceso anterior un prefijo, el cual dependerá de si lo recibe por anunciamiento de un router o no.
De esta manera si el nodo no recibe anunciamiento de prefijo por parte de un router usara por default el prefijo de enlace local (link local) igual a FE80 (1111 1110 1000 0000), este prefijo es de 16 bits por lo que los restantes 48 bits serán iguales a cero para completar los 64 bits de longitud del prefijo de red, es decir:
FE80:0000:0000:0000=FE80::/16
Por lo que agregando el prefijo de dirección link local a la representación del identificador de interfaz en notación hexadecimal separados por dos puntos la dirección IPv6 es:
FE80::**XX**XX:XXFF:FEXX:XXXX

- **Autoconfiguración stateless en ambientes donde si existen los ruteadores.**

La autoconfiguración stateless en presencia de ruteadores permite a un host generar sus propias direcciones usando una combinación de información disponible localmente e información anunciada por los routers.
Este mecanismo de autoconfiguración es implementada mediante el protocolo neighbor discovery (ND-descubrimiento de vecinos), con el cual cuando los equipos se conectan realizan peticiones solicitando el prefijo asignado a la subred en la que se encuentran, si existe un router conectado al segmento, este anuncia su prefijo que identifica a la subred asociada con el enlace, cuando el nodo recibe un prefijo por anunciamiento de router antepondrá este prefijo recibido al numero resultante de la manipulación que se hace de los caracteres hexadecimales que componen su dirección MAC para formar el identificador de interfaz
La dirección será formada por la combinación de ambos, el prefijo anunciado por el router y el identificador de interfaz. Por lo tanto si el identificador de interfaz es de 64 bits el prefijo de red (network prefix) tendrá 64 bits.
De esta manera el nodo autoconfigura la dirección de interenlace concatenando el prefijo de red recibido por un router advertisement que realiza el ruteador por multicast, al identificador de interfaz en formato EUI-64.
Este proceso es conveniente para entornos donde ninguna gestión administrativa es deseable. Este protocolo esta concebido especialmente para permitir una configuración sencilla de las direcciones
La autoconfiguración stateless requiere muy poca configuración en los ruteadores, y no requieren el uso de servidores adicionales. El problema de este tipo de autoconfiguración es

que debido a que no existe ningún control para la asignación de direcciones, el sistema será muy vulnerable a que cualquier persona ajena a la empresa llegue y se conecte a la red.
Un ruteador debe ser configurado por el administrador del sistema para poder controlar el mecanismo utilizado para la configuración de estaciones (con respecto a sus direcciones autoconfigurables). En un ruteador puede ser inicializada por el administrador para cada interfaz la siguiente variable:

Perform_Auto _Address: Si esta variable es puesta a TRUE (Valor por default), el ruteador manda una extensión de prefijo de dirección a todos los ruteadores de advertisement.

Procedimiento de autoconfiguración stateless de una interfaz.
Primeramente, solo las interfaces que so capaces de transmitir paquetes multicast (multicast-capable) se pueden autoconfigurar, por lo tanto los enlaces deben soportar trafico multicast. Cuando una interfaz se activa (por encendido o reinicio) el host genera una dirección de enlace local y es puesta en estado tentativo y se inicia el proceso de detección de dirección duplicada para determinar si esta en uso o no, si se determina su unicidad se asigna a la interfaz. Así este primer paso de autoconfiguración de la dirección de enlace local ejecutado tanto por hosts como por routers termina.
Los siguientes pasos son ejecutados solamente por los hosts. El paso que sigue es obtener un anunciamiento de router para verificar si existe o no un router en la red. Como los anunciamientos de router pueden ser en periodos largos, la interfaz puede mandar una solicitud de router a la dirección multicast de todos los routers FF02:2. Los anunciamientos de router contienen: dos banderas que indican el tipo de autoconfiguración ha ser usada, la bandera M (configuración de dirección administrada) indica si el host debe usar autoconfiguración stateful y la bandera O (otra configuración stateful) que indica si el host debe usar la autoconfiguración stateful para otra información los prefijos a ser usados para la autoconfiguración stateless de direcciones globales o de site local. Debido a la periodicidad de los anunciamientos de router las direcciones son continuamente actualizadas y nuevas direcciones pueden ser agregadas debido a la existencia de nuevos prefijos.

3.4.6.2 Autoconfiguración stateful

La autoconfiguración stateful se basa en el protocolo de configuración dinámica de hosts DHCP y en la existencia de un servidor dedicado a proporcionar las direcciones, parámetros y/o información de configuración que el equipo auto configurará. El servidor siempre mantendrá una base de datos para registrar las direcciones que han sido asignadas a los hosts.
Normalmente el servidor usara DHCP6 para poder realizar la función de proporcionar los parámetros necesarios a ser configurados a las interfaces de los equipos. La información proporcionada por DHCPv6 principalmente es direcciones IPv6, pero otros parámetros pueden ser proporcionados también.
El protocolo de configuración dinámica de las estaciones para IPv6 (DHCPv6). DHCPv6 es un protocolo más complejo que permite una asignación flexible de direcciones bajo el control del administrador del sistema. Este protocolo necesita un gestor de sistemas (servidor y bases de datos) importante.

Este tipo de configuración usa el esquema cliente servidor, los servidores administran las direcciones y la base de datos de parámetros de red y proporcionan a los clientes la elección de un procedimiento de configuración stateful.
Con este tipo de autoconfiguración se puede tener un mejor control administrativo pero tiene el detalle que requiere la presencia de servidores tanto DHCP6, como otros necesarios que proporcionen los parámetros necesarios para implementar el control y la configuración, además se tendrá que asignar previamente la dirección del o los servidores que proporcionen la información de configuración, con lo cual se pierde el esquema de autoconfiguración, ya que previamente habrá intervención manual.
Cuando un cliente usa la configuración stateful (especificada en el mensaje de anunciamiento de router) primero tiene que descubrir la dirección de un servidor DHCP que puede estar en otro enlace, para esto manda un mensaje multicast de Solicitud DHCP sobre su enlace y un servidor o relay responde con el mensaje de anunciamiento DHCP que contiene una o más direcciones unicast de direcciones de servidores DHCP.
Así el cliente puede adquirir parámetros de configuración mandando al servidor DHCP seleccionado un mensaje de petición DHCP y obtener un mensaje de respuesta DHCP.
Si el servidor debe reconfigurar al cliente, no lo hace directamente, sino que empieza una transacción a través de un mensaje de reconfiguración DHCP.
Uso combinado de autoconfiguración stateless y stateful.
Se pueden combinar los dos tipos de autoconfiguración, para lo cual el administrador deberá indicar en los campos apropiados del mensaje de anunciamiento de router que tipo de autoconfiguración se usará. Así primero por autoconfiguración stateless el equipo autoconfigura una dirección con la cual tiene conectividad a su segmento, una vez que tiene conectividad con los nodos conectados al mismo segmento, puede proceder a dialogar con el o los servidores para intercambiar los datos necesarios para implementar la autoconfiguración stateful.

Proceso de autoconfiguración de dirección en un nodo.
Una estación mantiene una lista de direcciones por interfaz, esta lista debe contener por lo menos una dirección de link local (intra-enlace) que puede formar automáticamente la estación cuando una interfaz sé inicializa. Si un ruteador esta conectado al enlace, la lista incluirá las direcciones de inter-enlace formados por prefijos de subred reclamados ya sea por peticiones a los ruteadores de advertisement o haciendo llamadas a DHCPv6. Las direcciones de interenlace también pueden configurarse manualmente.
La estación puede mantener una lista de las siguientes variables de configuración por interfaz:

- Dirección : una dirección unicast IPv6 valida en esta interfaz.. Por defecto: nada
- Tiempo de vida (life Time): el tiempo de vida en el cual la dirección es valida, medido en segundos. Por defecto: tiempo infinito. Para las direcciones de intra-enlace y todas las direcciones configuradas manualmente este tiempo de vida es puesto a infinito. Cuando tiempo de vida es fijado a un valor y este expira el enlace entre la dirección y la interfaz se vuelve invalido y la dirección puede ser reasignada a cualquier otro nodo en Internet. Las direcciones pueden estar en dos diferentes fases según su tiempo de vida: Preferido significa que el uso de la dirección en la comunicación no esta restringido y desaprobado es un anuncio de que la dirección se volverá invalida.

- Perform_Auto_Address: Una estación debe permitir al administrador del sistema configurar esta variable para cada interfaz. Si su valor es verdadero (TRUE) la estación deberá proceder a una configuración de direcciones automática y si su valor es (FALSE) no realizar ninguna autoconfiguración. El valor por default es TRUE.

Una estación debe realizar lo siguiente para cada interfaz cuando se arranca o cuando debe inicializarse una interfaz:

- Cuando una estación arranca o en cualquier momento en que no tiene ninguna dirección produce una dirección de intra-enlace y la añade a su lista de direcciones.
- La estación debe mandar una petición al ruteador (Router Solicitation), para realizar o verificar lo mas rápidamente posible sus direcciones de inter-enlace. Cuando es solicitado un ruteador de advertisement, la estación debe tratar la configuración de direcciones de la manera siguiente:

Si existe una extensión de prefijo de dirección, la estación forma o comprueba sus direcciones de inter-enlace autónomas. En caso contrario se debe usar el protocolo DHCPv6 para la autoconfiguración de las direcciones. Si no existe ninguna dirección por el interfaz, la estación pone en marcha una petición al servidor de DHCPv6 para adquirir una nueva dirección. Si por alguna razón DHCPv6 no lo consigue, la estación vuelve a utilizar una dirección de intra-enlace o una dirección de inter-enlace configurada manualmente hasta que logre la petición al servidor.

De esta forma con la característica de autoconfiguración, cada nodo puede configurar automáticamente su dirección IPv6. Sea cual fuere el tipo de dirección IPv6 que use un nodo, esta será autoconfigurada sin necesidad de la intervención directa de un administrador o incluso del mismo usuario. En el caso de direcciones especiales como las de túnel isatap o compatibles con IPv4, estas también serán autoconfiguradas por el nodo, solamente que en este caso se necesita tener una dirección IPv4 configuradas en el nodo para que el sistema autonfigure la dirección IPv6 en base a esa dirección IPv4.

Para la autoconfiguración de las direcciones v4-compatibles, el nodo debe poseer una dirección IPv4 sea privada o publica ya que IPv6 tomara esa dirección para autoconfigurar este tipo de direcciones en la forma:

::w.x.y.z

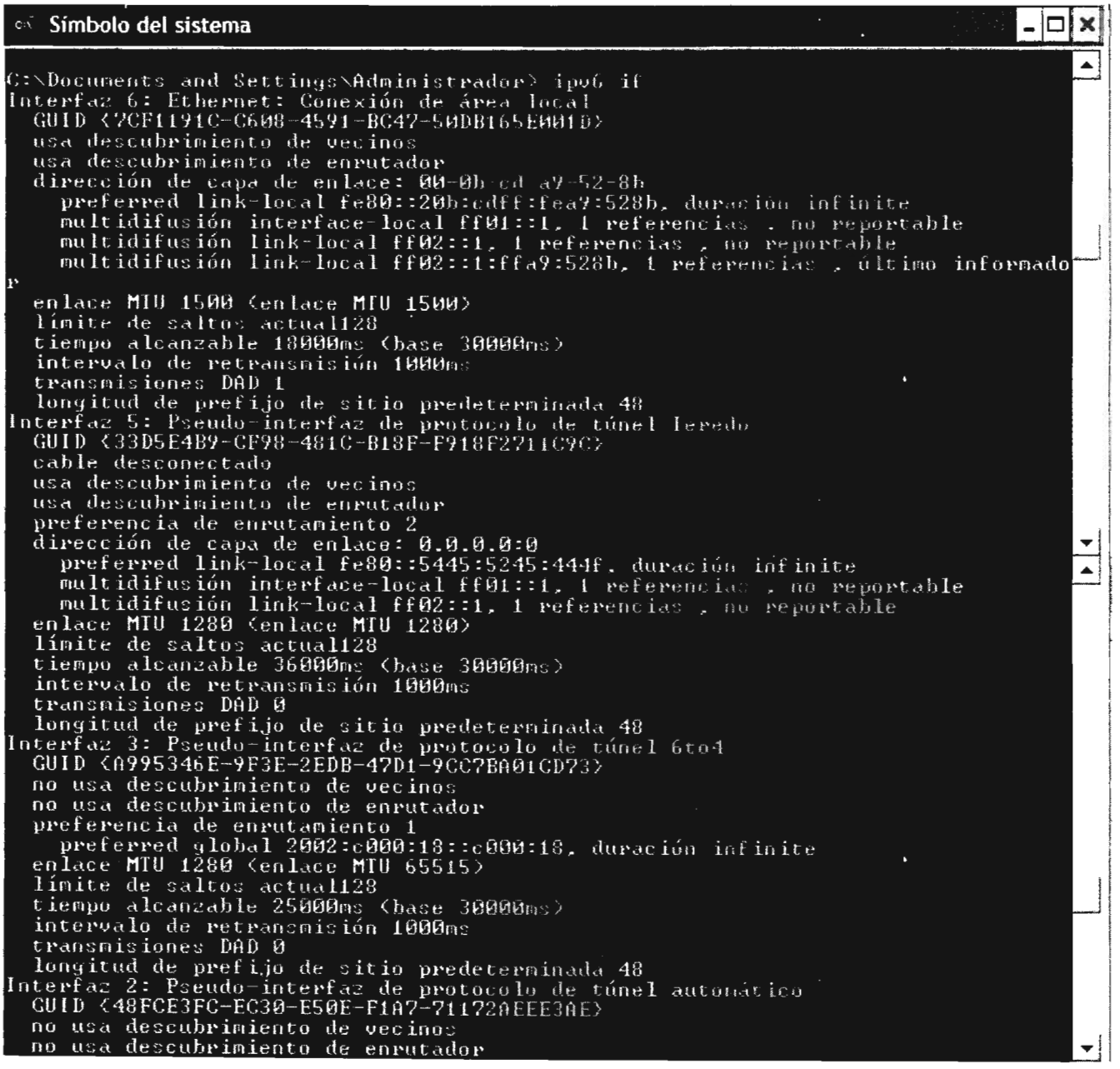
Donde:

w.x.y.z es la dirección IPv4 del nodo.

Para cualquier tipo de dirección que no sean del tipo link local o site local, debido a que en general deben tener conectividad o compatibilidad con IPv4 podemos decir que todas hacen un túnel puesto que encapsulan las direcciones IPv6 con encabezados IPv4 para poderse comunicar a través de redes IPv4 nativas.

Un nodo debe ejecutar un algoritmo de detección de dirección duplicada DAD para asegurarse que las direcciones configuradas son únicas en el enlace antes de asignarlas a una interfase, este algoritmo debe ser empleado independientemente de sí sé autoconfiguró la dirección vía un mecanismo stateless o stateful. El algoritmo DAD usa los mensajes de solicitud de vecino y anunciamiento de vecino para detectar direcciones duplicadas

En la figura 3.4.6.1 tenemos la pantalla de una estación a la cual se le instalo IPv6 y muestra la lista con las interfaces automáticas que aparecen por default:


Símbolo del sistema
C:\Documents and Settings\Administrador> ipv6 if
Interfaz 6: Ethernet: Conexión de área local
GUID {7CF1191C-C608-4591-BC47-50DB165E001D}
usa descubrimiento de vecinos
usa descubrimiento de enrutador
dirección de capa de enlace: 00-0b-cd a7-52-8b
preferred link-local fe80::20b:cdff:fea7:528b, duración infinite
multidifusión interface-local ff01::1, 1 referencias , no reportable
multidifusión link-local ff02::1, 1 referencias , no reportable
multidifusión link-local ff02::1:ffa7:528b, 1 referencias , último informado
enlace MTU 1500 (enlace MTU 1500)
límite de saltos actual128
tiempo alcanzable 18000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1
longitud de prefijo de sitio predeterminada 48
Interfaz 5: Pseudo-interfaz de protocolo de túnel Teredo
GUID {33D5E4B9-CF98-481C-B18F-F918F2711C9C}
cable desconectado
usa descubrimiento de vecinos
usa descubrimiento de enrutador
preferencia de enrutamiento 2
dirección de capa de enlace: 0.0.0.0:0
preferred link-local fe80::5445:5245:444f, duración infinite
multidifusión interface-local ff01::1, 1 referencias , no reportable
multidifusión link-local ff02::1, 1 referencias , no reportable
enlace MTU 1280 (enlace MTU 1280)
límite de saltos actual128
tiempo alcanzable 36000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48
Interfaz 3: Pseudo-interfaz de protocolo de túnel 6to4
GUID {A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
no usa descubrimiento de vecinos
no usa descubrimiento de enrutador
preferencia de enrutamiento 1
preferred global 2002:c000:18::c000:18, duración infinite
enlace MTU 1280 (enlace MTU 65515)
límite de saltos actual128
tiempo alcanzable 25000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48
Interfaz 2: Pseudo-interfaz de protocolo de túnel automático
GUID {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
no usa descubrimiento de vecinos
no usa descubrimiento de enrutador

Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrador> ipv6 if
Interfaz 6: Ethernet: Conexión de área local
GUID {7CF1191C-C608-4591-BC47-50DB165E001D}
usa descubrimiento de vecinos
usa descubrimiento de enrutador
dirección de capa de enlace: **00-0b-cd-a9-52-8b**
preferred link-local **fe80::20b:cdff:fea9:528b**, duración infinite
multidifusión interface-local ff01::1, 1 referencias , no reportable
multidifusión link-local ff02::1, 1 referencias , no reportable
multidifusión link-local ff02::1:ffa9:528b, 1 referencias , último informador
enlace MTU 1500 (enlace MTU 1500)
límite de saltos actual128
tiempo alcanzable 18000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 1
longitud de prefijo de sitio predeterminada 48
Interfaz 5: Pseudo-interfaz de protocolo de túnel Teredo
GUID {33D5E4B9-CF98-481C-B18F-F918F2711C9C}
cable desconectado
usa descubrimiento de vecinos
usa descubrimiento de enrutador
preferencia de enrutamiento 2
dirección de capa de enlace: 0.0.0.0:0
preferred link-local **fe80::5445:5245:444f**, duración infinite
multidifusión interface-local ff01::1, 1 referencias , no reportable
multidifusión link-local ff02::1, 1 referencias , no reportable
enlace MTU 1280 (enlace MTU 1280)

límite de saltos actual128
tiempo alcanzable 36000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48
Interfaz 3: Pseudo-interfaz de protocolo de túnel 6to4
GUID {A995346E-9F3E-2EDB-47D1-9CC7BA01CD73}
no usa descubrimiento de vecinos
no usa descubrimiento de enrutador
preferencia de enrutamiento 1
preferred global **2002:c000:18::c000:18**, duración infinite
enlace MTU 1280 (enlace MTU 65515)
límite de saltos actual128
tiempo alcanzable 25000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48
Interfaz 2: Pseudo-interfaz de protocolo de túnel automático
GUID {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
no usa descubrimiento de vecinos
no usa descubrimiento de enrutador
preferencia de enrutamiento 1
Dirección IPV4 incrustada EUI-64: 0.0.0.0
dirección de capa de enlace de enrutador: 0.0.0.0
preferred link-local **fe80::5efe:192.0.0.24**, duración infinite
enlace MTU 1280 (enlace MTU 65515)
límite de saltos actual128
tiempo alcanzable 18000ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48
Interfaz 1: Pseudo-interfaz de bucle invertido
GUID {6BD113CC-5EC2-7638-B953-0B889DA72014}
no usa descubrimiento de vecinos
no usa descubrimiento de enrutador
dirección de capa de enlace:
preferred link-local ::1, duración infinite
preferred link-local fe80::1, duración infinite
enlace MTU 1500 (enlace MTU 4294967295)
límite de saltos actual128
tiempo alcanzable 41500ms (base 30000ms)
intervalo de retransmisión 1000ms
transmisiones DAD 0
longitud de prefijo de sitio predeterminada 48

Fig. 3.4.6.1 Captura de las direcciones autoconfiguradas en un equipo con IPv6

3.4.7 Renumeración de routers

El mecanismo de renumeración de routers permite que los prefijos de dirección de los routers sean configurados y reconfigurados casi tan fácilmente como la combinación de descubrimiento de vecinos y la autoconfiguración de direcciones trabajan para los hosts.
Recordemos que el descubrimiento de vecinos y la autoconfiguración de dirección realizan las asignaciones iniciales de prefijos de dirección a los hosts y estos dos mecanismos también simplifican la reconfiguración de hosts cuando los prefijos validos cambian.
El mecanismo de renumeración de router proporciona un medio para que el administrador de red realice actualizaciones a los prefijos usados por los routers IPv6 y anunciados por los routers IPv6 a lo largo de un sitio.
La renumeración de routers ejecuta una secuencia de Operaciones de Control de Prefijo PCO (Prefix Control Operations), las operaciones pueden ser:

- ADD: La operación ADD indica al router que agregue los prefijos-a-usar (Use-Prefixes) al conjunto de prefijos configurados.
- CHANGE: La operación CHANGE indica al router que remueva el prefijo que corresponde al prefijo-de-correspondencia (Match-Prefix) y lo reemplace con los prefijos-a-usar.
- SET-GLOBAL: La operación SET-GLOBAL indica al router que reemplace todos los prefijos globales con los prefijos-a-usar.

Los routers procesan cada PCO checando cada una de sus interfaces para hallar una dirección o prefijo que corresponda al prefijo-de-correspondencia.

Renumeración de sitios
Los protocolos de capas superiores realizan conexiones usando la dirección IP, por lo que un cambio de dirección puede interrumpir las conexiones en progreso, esto puede hacer a la renumeración un tanto complicada y delicada, pero en IPv6 se simplifica.
Para entender esto partamos de que las direcciones se dividen en direcciones validas e invalidas. A su vez las direcciones validas se subdividen en direcciones preferidas y desaprobadas.
De esta forma las nuevas conexiones de los protocolos de capas superiores deben ser abiertas usando siempre direcciones preferidas, ya que cuando los administradores de red empiezan el procedimiento de renumeración primero insertan los nuevos prefijos en los routers y esperan a que el DNS los propague en la red entera, después de algunos días los administradores remueven los viejos prefijos de direcciones que ya no serán usadas.
Este procedimiento crea nuevas direcciones preferidas en todas las interfaces y transforma algunas direcciones que antes eran preferidas en desaprobadas. La dirección permanece en estado desaprobado por un tiempo razonable para que las conexiones abiertas cuando la dirección era preferida sean cerradas correctamente, ya que aunque las direcciones desaprobadas siguen siendo validas, no pueden ser abiertas nuevas conexiones con ellas. Posteriormente las direcciones desaprobadas se vuelven invalidas y la transición de las anteriores direcciones a las nuevas termina. En la fase de transición los routers deben anunciar ambas direcciones.

Multihoming

Multihoming es la conexión de un sitio a mas de un proveedor de servicios de Internet ISP (Internet Service Provider) para propósitos de redundancia y balanceo de carga, Fig. 3.4.7.1.

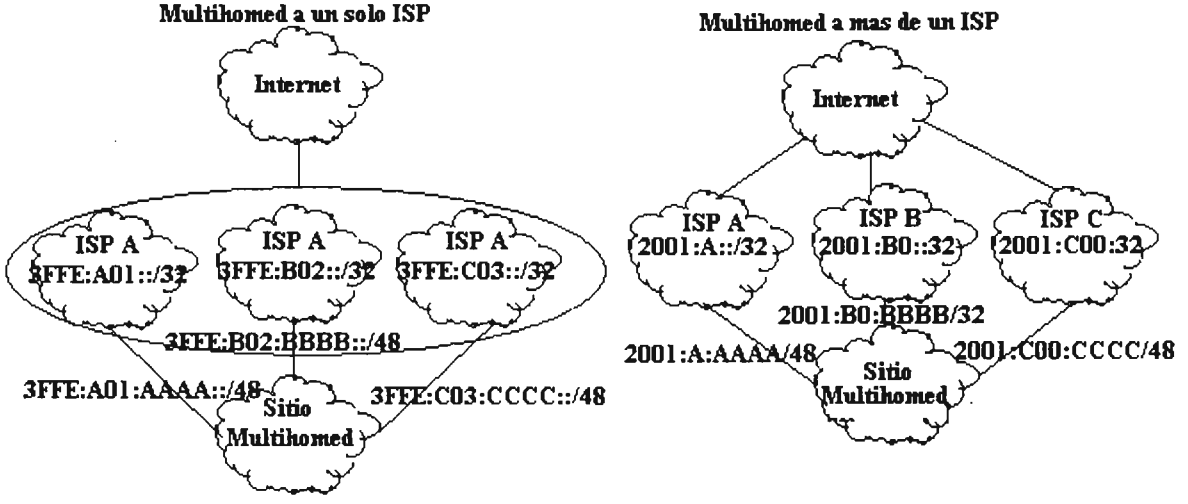


Fig. 3.4.7.1 Multihoming

La conexión a diferentes sitios usa los protocolos de ruteo existente y las implementaciones existentes por lo que no se requieren nuevos protocolos o cambios.

Hay dos tipos de conexiones multihoming:

- Sitio multihomed conectado a un solo ISP en diferentes puntos geográficos.
- Sitio multihomed conectado a mas de un ISP.

Las rutas que se asocian al sitio multihomed no son vistas desde el exterior del ISP, por lo que no hay un impacto real en el ruteo global. El sitio multihomed obtendrá direcciones IP designando a uno de sus ISPs como el ISP primario, recibiendo de esta forma la asignación de dirección IP del bloque de agregación IPv6 del ISP primario.

3.4.8 Mecanismos de transición a IPv6 y coexistencia con IPv4

Debido a que la infraestructura actual de Internet es enorme, los protocolos y servicios implementados sobre esta son innumerables y todo esto funciona sobre IPv4, por lo que se hizo necesario definir junto con la propuesta de IPv6 estrategias adecuadas para realizar la integración entre ambos protocolos manteniendo la coexistencia con IPv4.

La transición de IPv4 a IPv6 se conforma de un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición con la menor interrupción posible.

Para realizar la transición de los sistemas IPv4 a IPv6 se han propuesto varias técnicas las cuales son englobadas en un solo conjunto conocido como SIT (Simple Internet Transition).

Este sistema de transición hace mucho hincapié en que el proceso de transición sea fácil desde el punto de vista del administrador y del usuario.

Las principales características de SIT son:

- Transición progresiva. Los hosts y routers pueden ser actualizados uno a la vez, sin que los otros sean actualizados simultáneamente.
- Mínimos requerimientos de actualización. El único requisito para administrar hosts a IPv6 es la disponibilidad de un servidor DNS para manejar direcciones IPv6.
- Simplicidad de direccionamiento. Cuando un host o router es actualizado a IPv6 puede continuar usado direcciones IPv4.
- Bajo costo inicial. No es necesario ningún trabajo preparatorio para empezar a migrar a IPv6.

La transición tiene dos grandes características: la compatibilidad y la interoperabilidad.
La compatibilidad asegura que las inversiones actuales en IPv4 están seguras.
La interoperabilidad asegura que la transición es gradual y no impacta el funcionamiento actual de Internet.
Se recomienda instalar IPv6 primeramente en el borde de la red y posteriormente realizar lo propio con el núcleo de la red para reducir los costos e impactos operacionales de la integración. Las estrategias clave para instalar IPv6 en los bordes de una red incluyen transportar trafico IPv6 sobre la red IPv4, permitir a los dominios de IPv6 aislados comunicarse con cada uno de los otros antes de la transición completa a un backbone de IPv6 nativo, correr IPv4 e IPv6 a lo largo de la red, desde todos los bordes a través del núcleo, o traducir entre IPv4 e IPv6 para permitir a los hosts comunicarse transparentemente con un protocolo con hosts corriendo el otro protocolo. Todas las técnicas, estrategias o mecanismos permiten a las redes ser actualizadas e IPv6 instalado incrementalmente con poca o nula interrupción de los servicios IPv4.
En forma genérica los mecanismos usados por el SIT para la migración a IPv6 son:

- Una estructura de direcciones IPv6 que permita derivar las direcciones IPv6 de las direcciones IPv4.
- Disponibilidad de la doble pila en hosts y routers durante la transición, o sea, el manejo de tanto la pila IPv4 como la pila IPv6 al mismo tiempo.
- Una técnica para encapsular paquetes IPv6 dentro de paquetes IPv4, técnica conocida también como tunneling, que permita a los paquetes IPv6 atravesar redes IPv4.
- Una técnica opcional que traduzca encabezados IPv6 en encabezados IPv4 y viceversa, que permita una fase avanzada de la migración donde nodos IPv4-nativos se puedan comunicar con nodos IPv6-nativos.

Algunas técnicas para llevar a cabo esta transición son:

- Instalación de doble pila (IPv4 e IPv6) en los hosts y routers que deben interoperar entre IPv4 e IPv6.
- Implementación de IPv6 sobre backbones de doble pila. Con esta técnica las aplicaciones IPv4 e IPv6 pueden coexistir en un backbone de ruteo de doble capa IP. Todos los routers o una porción de ellos, serán actualizados para manejar una doble pila (los routers de acceso (CPE) y los routers de agregación, los del núcleo permanecen igual), de esta forma la comunicación con IPv4 usa la pila del protocolo IPv4 y la comunicación con IPv6 usa la pila IPv6.
  Las técnicas de doble pila permiten la coexistencia tanto de IPv4 como de IPv6 en los mismos dispositivos y redes.
- Implementación de un mecanismo de túneles de IPv6 sobre IPv4. La topología de IPv6 inicial es construida con túneles sobre IPv4. El túnel permite la creación de

nodos solo IPv6, que deben existir en redes IPv6 completamente funcionales. Los túneles encapsulan el trafico IPv6 dentro de los paquetes IPv4, inicialmente permiten la comunicación entre sitios IPv6 aislados o conexión a redes IPv6 remotas sobre un backbone IPv4. Los túneles puede ser túneles manualmente configurados, túneles de encapsulamiento de ruteo genérico (GRE), túneles semiautomáticos como los servicios de túneles brokers, mecanismos de túneles totalmente automáticos como 6to4 para la WAN y el protocolo de direccionamiento de túnel automático intrasitio ISATAP(Intrasite Automatic Túnel Addressing Protocol) para un ambiente de campus.
Las técnicas de tunelización evitan las dependencias cuando se actualicen hosts routers o regiones.

- Direcciones IPv4 contenidas en IPv6. Para ello a los hosts IPv6 se les asignan direcciones compatibles con IPv4 y las direcciones IPv4 se mapean a IPv6, este mecanismo es mas comúnmente conocido como direcciones compatibles con IPv4.
- Instalación de IPv6 sobre enlaces de datos dedicados. Este mecanismo permite la comunicación de los dominios IPv6 usando la misma infraestructura de capa 2 de IPv4, pero con IPv6 usando circuitos virtuales permanentes (PVCs) Frame Relay o ATM, enlaces ópticos separados, o DWDM.
- Instalación de IPv6 sobre backbones MPLS (Multiprotocol Label Switching). Con este mecanismo los dominios aislados IPv6 se pueden comunicar con cada uno de los otros sobre un backbone IPv4 MPLS sin modificar la infraestructura del núcleo. Muchas técnicas están disponibles en diferentes puntos en la red con pocos cambios a la infraestructura del backbone o reconfiguración de los routers del núcleo debido a que el envío se basa en etiquetas mas que en el encabezado en sí mismo.
- Uso de mecanismos de traducción de cabeceras de protocolo IPv4/IPv6 en los routers situados entre redes IPv4 e IPv6.
  Las técnicas de traducción de cabeceras permiten a los dispositivos IPv6-nativos comunicarse con dispositivos IP4-nativos.

Estas técnicas se pueden adaptar a otros protocolos como CLNP e IPX que tienen semánticas similares a nivel de red y sus esquemas de direccionamiento son maleables a IPv6.
La transición se ha planteado como una migración de las diferentes organizaciones de forma independiente y en dos fases.
La primer fase de la transición se compone de los siguientes mecanismos básicos:

- Uso de ambos protocolos IPv4 e IPv6 (doble pila IPv6/IPv4).
- Uso de túneles IPv6 en IPv4.
- Uso de direcciones compatibles con IPv4.
- Traducción de cabeceras.

3.4.8.1 Uso de ambos protocolos IPv4 e IPv6 (doble pila IPv6/IPv4).

Esta es la etapa de migración hacia una infraestructura doble IPv6/IPv4 (Dual stack IPv6/IPv4).
En esta fase se proporciona soporte completo para IPv4 e IPv6 en hosts y routers, es decir se usan simultáneamente en un nodo ambos protocolos.

Esta estrategia se basa en el ruteo tanto de IPv4 como de IPv6. Por lo que todos los routers en la red deberán ser actualizados para manejar la doble pila.
Esta primera fase debiera ser más fácil, ya que todos los nodos soportan IPv4.
Los sistemas finales con doble pila permiten que las aplicaciones se migren una a la vez de IPv4 a IPv6.
La mejor forma para que los nodos IPv6 sean compatibles con nodos IPV4-nativo es conteniendo una implementación completa de IPv4. Los nodos que poseen una implementación completa de IPv4 además de su implementación de IPv6 son llamados nodos IPv6/IPv4. Estos nodos tienen la capacidad de enviar y recibir paquetes IPV6 e IPv4, de esta forma pueden interoperar directamente con nodos IPv4 usando paquetes IPv4 y también pueden operar con nodos IPv6 usando paquetes IPv6.

Instalación de la doble pila IPv6/IPv4
Esta fase implica reemplazar el software de nodos solo IPv4 por software IPv6/IPv4. Es decir al instalar IPv6 en un sistema no se debe quitar el protocolo IPv4. Esto debería ser parte de los ciclos habituales y los nodos IPv4 continuarían funcionando en modo compatible con IPv6. En el caso de nuevas versiones de sistemas operativos IPv6 ya viene incluida, por lo que no tendrá un costo adicional.
El tener una pila dual establece una duplicidad en los protocolos de la capa de red. Por su parte se requieren los cambios pertinentes en los protocolos de transporte para trabajar con ambas pilas, sucede lo mismo con las aplicaciones si se pretende que exploten las posibilidades de IPv6 como por ejemplo la mayor longitud de las direcciones.
Para que dos nodos IPv4 e IPv6 puedan interactuar dependen de sus capacidades y direcciones, así:

- Un nodo IPv6 con una dirección compatible con IPv4 puede interoperar directamente con otros nodos.
- Un nodo solo IPv6 con una dirección compatible de IPv4 puede interoperar con el resto de los nodos pero necesitara un router para traducir las cabeceras IPv6 a IPv4 y viceversa para poder operar con nodos IPv4.
- El nodo IPv6 con solo direcciones IPv6 no puede operar con nodos IPv4.
- El nodo solo IPv4 puede interoperar directamente con nodos IPv6/IPv4 con direcciones compatibles con IPv4.
- El nodo solo IPv4 puede interoperar con nodos solo IPv6 que tengan direcciones compatibles con IPv4, pero necesitara un router para traducir las cabeceras IPv4 a IPv6 y viceversa.
- El nodo IPv4 no puede interoperar con nodos IPv6 que tengan direcciones solo IPv6.

Las aplicaciones que no son actualizadas para soportar IPv6 pueden coexistir con las aplicaciones actualizadas en el mismo sistema final. Con esta estrategia las aplicaciones simplemente hacen uso de ambas pilas de protocolos. Fig. 3.4.8.1.1.

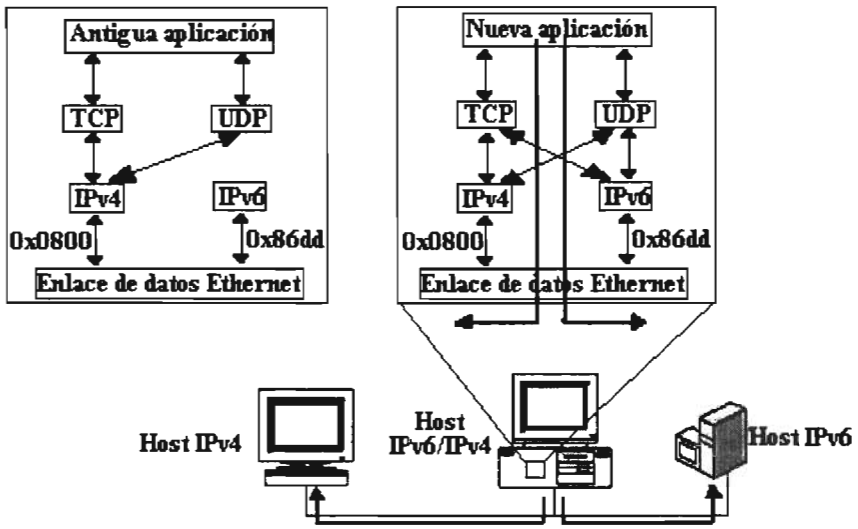


Fig. 3.4.8.1.1 Manejo de doble pila IPv4/IPv6

En la Fig. 3.4.8.1.1 se puede observar que las aplicaciones nuevas y actualizadas usan ambas pilas de protocolos IPv4 e IPv6. Para esto una nueva interfaz de programación de aplicación API (aplication- programming interface) se definió para poder manejar ambas direcciones IPv4 e IPv6 y solicitudes DNS. La aplicación que se actualiza con la nueva API puede seguir usando la pila del protocolo IPv4.

La forma de operar del enfoque de doble pila es:

- Si la dirección destino usada por la aplicación es una dirección IPv4, entonces la pila de protocolos IPv4 es usada.
- Si la dirección destino usada por la aplicación es una dirección IPv6 con dirección IPv4 insertada, entonces IPv6 es encapsulado dentro de IPv4
- Si la dirección destino es una dirección IPv6 de otro tipo, entonces IPv6 es usado, posiblemente encapsulado en el túnel configurado por default.

Los requisitos clave de esta estrategia son que cada sitio tenga un prefijo IPv6 unicast global y entradas apropiadas en un DNS que han el mapeo entre nombres de host y direcciones IP tanto para IPv4 como para IPv6.

Las aplicaciones decidirán entre usar IPv4 o IPv6 en base a la búsqueda de nombres, el tipo de trafico IP y los requerimientos de comunicación. Para esto la aplicación solicita todas las direcciones disponibles para un nombre de host, en muchos casos las direcciones IPv6 son las elecciones por default. Así las aplicaciones o librerías decidirán que versión de IP usar en base a:

- Cuando inician la comunicación y solicitan la resolución de nombres a un DNS, si el DNS tiene un registro AAAA o A6 usaran IPv6, si tiene un registro A usaran IPv4. Para usar IPv6 el nodo debe determinar si tiene conectividad IPv6 directa, de lo contrario deberá transmitir el paquete IPv6 en un túnel IPv4 siempre y cuando el nodo pueda usar túneles.
- Cuando responden a la comunicación iniciada por otra aplicación se basaran en la versión del paquete iniciador.

Este enfoque de doble pila permite la coexistencia indefinida de IPv4 e IPv6, además de una actualización gradual aplicación, por aplicación hacia el uso de IPv6.

El ruteo de doble pila es una estrategia para infraestructuras con una mezcla de aplicaciones IPv4 e IPv6 (como un campus o un punto de agregación de presencia) que requieren que ambos protocolos sean configurados. Pero aparte de que se tienen que actualizar todos los routers en la red, se requiere un esquema de direccionamiento doble, una administración doble de los protocolos de ruteo IPv4 e IPv6 y los equipos deben tener suficiente memoria para manejar las tablas de ruteo tanto de IPv4 como de IPv6. Asimismo se requiere seguir usando direcciones IPv4.

- **Implementación de IPv6 sobre backbones de IPv6.**

Con la instalación del backbone de doble pila, los routers de la red deben ser actualizados para ser de doble pila. De esta forma la comunicación IPv4 usara la pila del protocolo IPv4 con transmisión de paquetes IPv4 en base a las rutas aprendidas con protocolos de ruteo IPv4 y la comunicación IPv6 usara la pila IPv6 con rutas aprendidas con los protocolos de ruteo IPv6. Por su parte las aplicaciones se basaran en la respuesta del DNS para seleccionar entre usar IPv4 o IPv6 en base al tipo de trafico IP y los requerimientos de comunicación, Fig. 3.4.8.1.2.

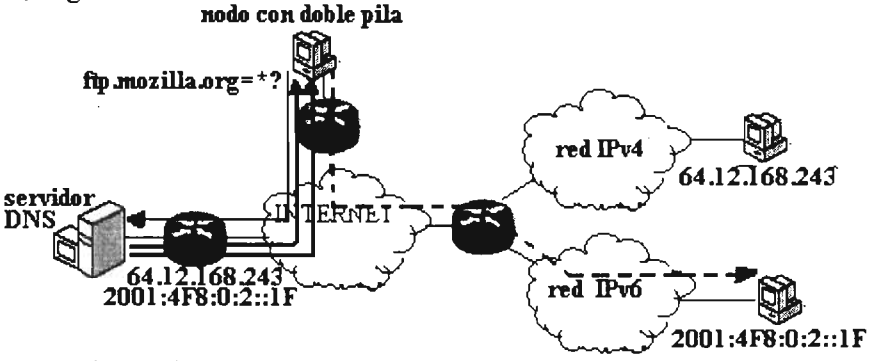


Fig. 3.4.8.1.2. Selección de la pila IP en base a la respuesta del DNS

Los routers ademas de que deben ser actualizados, necesitaran la configuración de un esquema de direccionamiento doble, doble administración de los protocolos de ruteo IPv4 e IPv6 y deben ser configurados con suficiente memoria para que puedan manejar ambas tablas de ruteo IPv4 e IPv6.

3.4.8.2 Implementación de un mecanismo de túneles IPv6 sobre IPv4.

El uso de túneles es una de las estrategias clave tanto para proveedores de servios como empresas durante el periodo de coexistencia entre IPv4 e IPv6. El mecanismo de tunneling encapsula paquetes IPv6 con encabezados IPv4 (o tramas MPLS) para formar datagramas IPv4 que pueden ser fragmentados los cuales son transportados a través de un backbone IPv4 o la infraestructura de ruteo Internet IPv4. Es decir el uso de túneles permitirá la circulación del trafico IPv6 a través de routers que no manejan IPv6. Con el uso de túneles los sistemas finales y routers IPv6 aislados se pueden comunicar entre sí o con otras redes IPv6 como el 6BONE sin la necesidad de actualizar la infraestructura IPv4 existente entre ellos, con lo cual los servicios IPv4 actuales no serán impactados, Fig. 3.4.8.2.1.

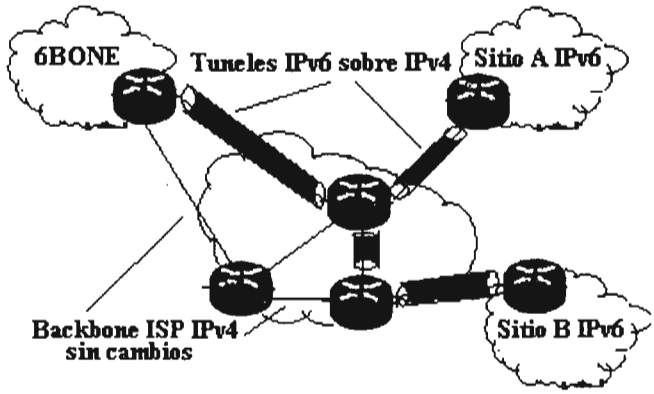


Fig. 3.4.8.2.1 Empleo de túneles sobre la infraestructura IPv4

El mecanismo de túnel se muestra en la Fig. 3.4.8.2.2.

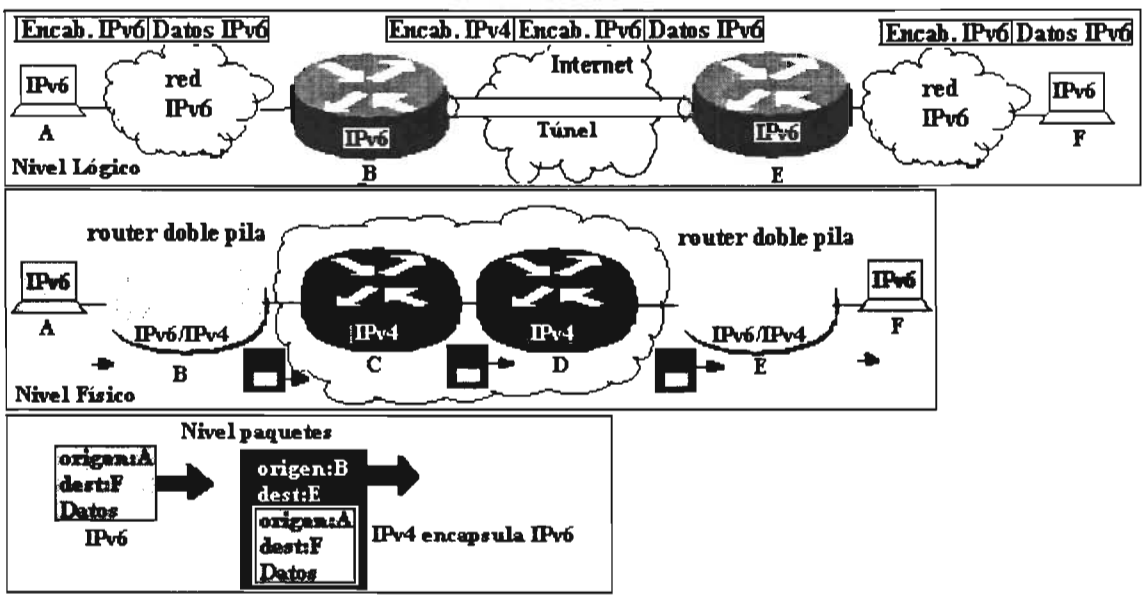


Fig. 3.4.8.2.2 Mecanismo de Tunneling

Los mecanismos de túneles requieren que los puntos extremos de un túnel manejen ambas pilas de protocolo IPv4 e IPv6, asi los routers pueden interoperar directamente tanto con sistemas finales y routers IPv4 como con sistemas finales y routers IPv6. Para la correcta operación del túnel se deben tener las entradas en un DNS que mapeen los nombres de hosts y direcciones IP tanto para IPv4 como para IPv6 para que las aplicaciones puedan seleccionar la dirección requerida.

En este periodo de transición en el que IPv6 e IPv4 deberán coexistir existe una variedad de mecanismos de túneles, estos se clasifican en dos grandes tipos por su forma de creación:

- Túneles configurados
- Túneles automáticos.

Estos túneles configurados y automáticos se pueden clasificar según los elementos extremos que los crean:

- Túneles entre routers IPv6/IPv4. Para crear este túnel los dos routers extremos con doble pila IPv6 toman de su red interna el trafico IPv6 lo encapsulan para

realizar el envío por el Internet IPv4 y cuando reciben el paquete encapsulado quitan el encabezado IPv4 y dejan pasar el paquete IPv6 hacia su destino, Fig. 3.4.8.2.3.

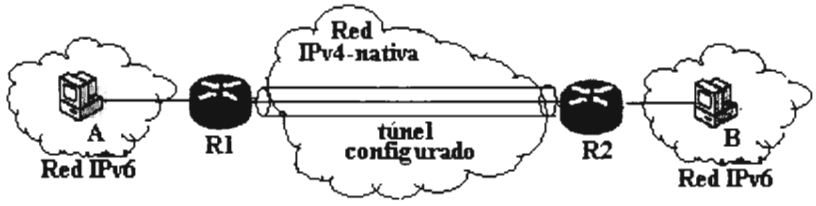


Fig. 3.4.8.2.3 Túnel configurado router a router.

Aquí el paquete es tunelizado a un router, por lo que el punto final de este tipo de túnel es un router. No hay relación entre la dirección de router y la dirección del destino final, por lo que la dirección del router que es el punto final del router debe ser manualmente configurada, creándose de esta manera un túnel configurado.

- Túneles entre computadora IPv6/IPv4 y router IPv6/IPv4 (host a router). Este túnel es creado por un nodo con doble pila que encapsula el trafico en un datagrama IPv4 para enviarlo a través de la infraestructura IPv4, en el otro extremo un router con doble pila recibe el datagrama IPv4 desencapsula el paquete IPv6 y lo entrega a una red nativa de IPv6, Fig. 3.4.8.2.4.

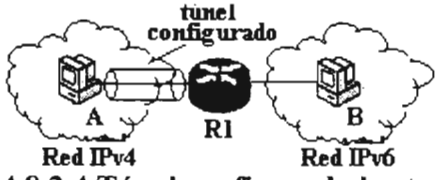


Fig. 3.4.8.2.4 Túnel configurado host a router

El paquete es tunelizado a un router, por lo que el punto final de este tipo de túnel es un router. No hay relación entre la dirección de router y la dirección del destino final, por lo que la dirección del router que es el punto final del router debe ser manualmente configurada, creándose de esta manera un túnel configurado.

- Túneles entre computadoras IPv6/IPv4 (host a host). Los nodos con la doble pila se comunican a través de la infraestructura de IPv4 encapsulando el trafico IPv6 en IPv4. Fig. 3.4.8.2.5.

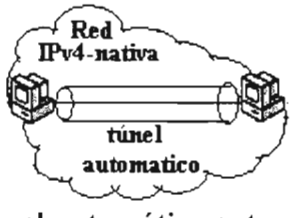


Fig. 3.4.8.2.5 Túnel automático entre hosts IPv6/IPv4.

En este caso el paquete IPv6 es tunelizado de un host a su host destino, por lo que la dirección de punto final del túnel y la dirección del host destino es la misma. Si la dirección IPv6 usada por el destino es compatible con IPv4, la dirección IPv4 del punto final del túnel se deriva de la dirección IPv6, no requiriendo configuración manual, es un túnel automático.

- Tuneles de router a host IPv6/IPv4. Los routers IPv6/IPv4 pueden usar la infraestructura IPv4 para alcanzar un host IPv6/IPv4., Fig. 3.4.8.2.6.

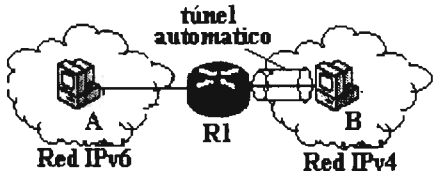


Fig. 3.4.8.2.6 Túnel de router a host IPv6/IPv4

El paquete IPv6 es tunelizado de un host a su host destino, por lo que la dirección de punto final del túnel y la dirección del host destino es la misma. Si la dirección IPv6 usada por el destino es compatible con IPv4, la dirección IPv4 del punto final del túnel se deriva de la dirección IPv6, no requiriendo configuración manual, es un túnel automático.

De esta manera los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Los paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6.

Los túneles IPv6 sobre IPv4 pueden ser vistos como si IPv6 fuera una red VPN (Virtual private Network) sobre Internet IPv4, o como que IPv6 usa a IPv4 como una capa de enlace virtual.

El uso de routers para entablar la comunicación es preferido sobre el tunneling por las siguientes razones:

- Hay menos overhead pues no se requiere hacer encapsulación con cabeceras IPv4.
- Solo están disponibles características de IPv6.
- La topología de ruteo IPv6 se usara desde su instalación preferentemente a la de IPv4.

Dentro de esta clasificación general tenemos las siguientes técnicas de túneles:

- Túneles manualmente configurados.
- Túneles de encapsulamiento de ruteo genérico (GRE) IPv6 sobre IPv4.
- Túneles semiautomáticos como los servicios de túneles brokers, que proporcionan proveedores de servicio.
- Mecanismos de túneles totalmente automáticos como túneles 6to4 para la WAN, túneles compatibles-IPv4, el protocolo de direccionamiento de túnel automático intrasitio ISATAP(Intrasite Automatic Túnel Addressing Protocol) para un ambiente de campus, 6over4 crea un túnel intra-dominio que usa el multicast IPv4 como una LAN virtual.

3.4.8.2.1 Túneles manualmente configurados.

Un túnel manualmente configurado es equivalente a un enlace permanente entre dos dominios IPv6 sobre el backbone IPv4.

Los túneles configurados proporcionan conexiones estables y seguras entre dos routers de frontera de la red o entre sistemas finales y un router de frontera o para conectarse a redes IPv6 remotas.

Los túneles configurados son creados mediante configuración manual como en el caso de la red IPv6 6Bone. Este proceso se usa para realizar tunneling de host a router o de router a router de IPv6 sobre IPv4 estos routers o host deben ser de doble pila.

Los túneles manuales son configurados entre dos puntos finales que manejan ambas pilas (IPv6/IPv4) y requieren la configuración tanto de las direcciones fuente como las direcciones destino IPv4 e IPv6 del túnel.
Este tipo de túneles se pueden configurar entre dos hosts, entre un host y un router y entre dos routers, Fig. 3.4.8.2.1.1.

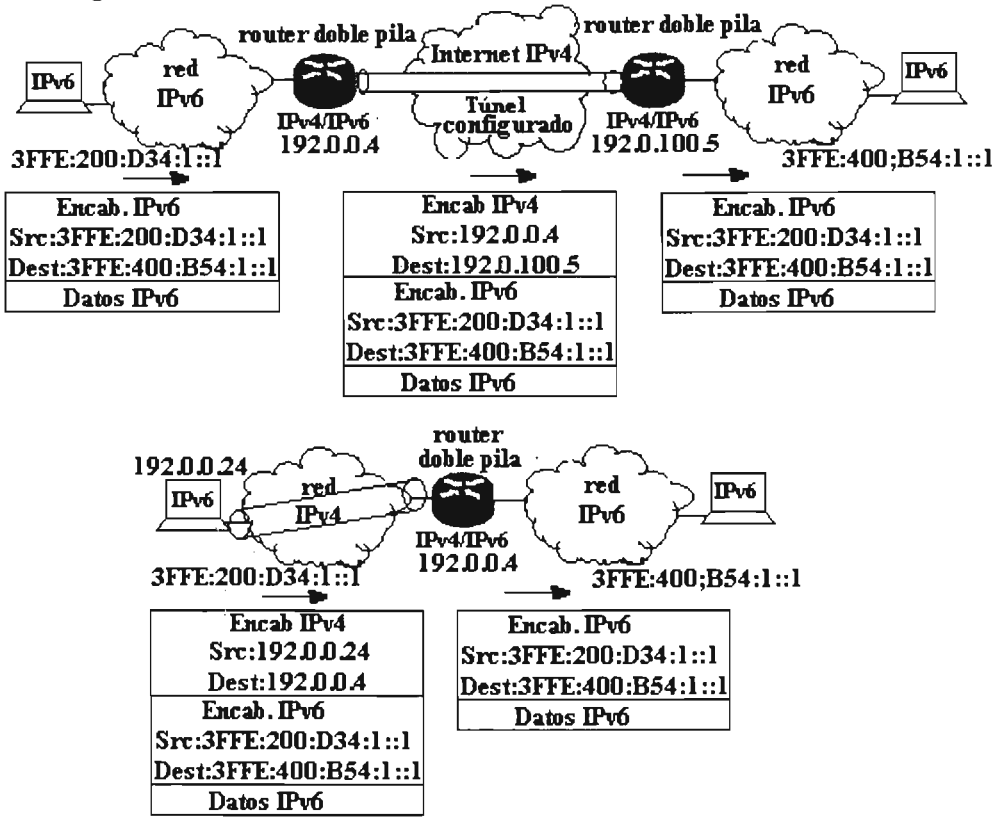


Fig. 3.4.8.2.1.1 Túnel manualmente configurado

En cada extremo del túnel se configuran las direcciones IPv4 e IPv6 del nodo de doble pila sobre la interfaz túnel. Para las empresas, el ISP les proporciona el prefijo de la dirección IPv6 del sitio, también proporciona la dirección IPv4 destino del punto de salida del túnel.
Estos túneles requieren contar con una dirección IPv4 globalmente ruteable.
El host emisor o router retransmisor se configuran de tal forma que la ruta además de contar con el siguiente salto, tiene una dirección de fin de túnel (esta dirección de fin de túnel es compatible con IPv4 ya que es un host IPv6/IPv4). El proceso de encapsulación viene a ser el mismo que en modo automático solo que la dirección IPv4 de destino no se calcula de los 32 bits inferiores de la dirección IPv6, sino de los 32 bits inferiores del fin de túnel. Cuando el router del fin del túnel recibe el datagrama lo procesa como un nodo que estaría al final del túnel automático. Cuando el paquete IPv6 original pasa a la capa IPv6 del router este reconoce que no es el destinatario y lo retransmite como lo haría con cualquier paquete IPv6.
El uso de traducción de direcciones NAT no es permitido a lo largo de la ruta de un tunel.

3.4.8.2.2 Túnel GRE IPv6 sobre IPv4

El túnel de encapsulamiento de ruteo genérico GRE (Generic Routing Encapsulation) IPv6 sobre IPv4 implementa un esquema de encapsulamiento estandar punto a punto. Estos túneles son enlaces entre dos puntos con un túnel separado por cada enlace. Los túneles GRE no están atados a un protocolo de transporte o pasajero especifico, en este caso transportan trafico IPv6 como el protocolo pasajero sobre GRE como el protocolo portador, Fig. 3.4.8.2.2.

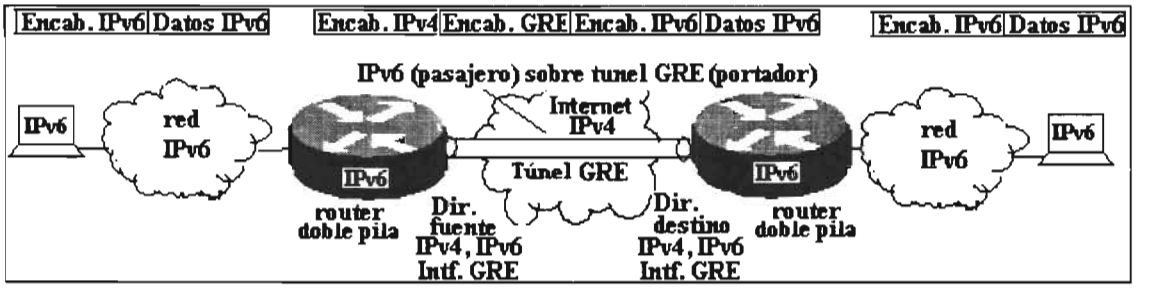


Fig. 3.4.8.2.2 IPv6 sobre túnel GRE.

Estos túneles requieren la configuración de las direcciones fuente y destino del túnel. Los routers de borde y sistemas finales usados como extremos del túnel deben ser dispositivos de doble pila. Se configuran las direcciones IPv4 e IPv6 del router de doble pila sobre la interfaz túnel GRE y se identifican los puntos de entrada y salida (fuente y destino) del túnel., usando direcciones IPv4.

3.4.8.2.3 Uso de túneles brokers o intermediaros.

Un servicio túnel broker permite a las aplicaciones IPv6 sobre sistemas finales de doble pila remotos o que están conectados a routers de doble pila accesar al backbone IPv6.
Algunas organizaciones que fungen como intermediarios entre islas IPv6 y la red IPv6 a través de Internet IPv4 permiten establecer túneles con su servidor de túneles para que de esta manera nuestro trafico IPv6 generado pase por su servidor de túneles y de ahí se redireccione a la red IPv6, Fig. 3.4.8.2.3.1.

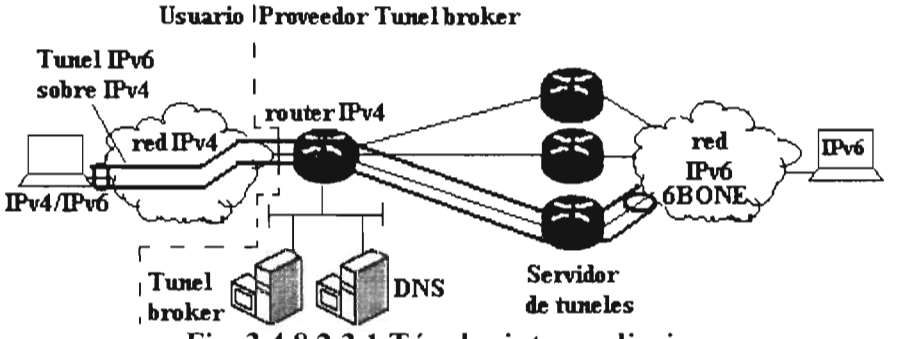


Fig. 3.4.8.2.3.1 Túneles intermediarios

Los túneles brokers son empresas proveedoras de túneles que proporcionan servicios de conectividad a la red IPv6 de pruebas 6BONE. Los túneles broker usan un servicio basado en Web para crear un túnel semiautomatizado.

El túnel broker usa túneles 6over 4 para conectar los sistemas finales al backbone IPv6.
La primera generación de servicio túnel broker consistía en un servidor Web que administra las peticiones de túneles de los clientes, el proveedor de túnel broker genera el túnel para la empresa y manda la información del regreso al cliente, configura nuestro servidor o router, automatiza la configuración manual de túneles (con direcciones IPv4 fuente y destino explicitas y direcciones fuente y destino IPv6) sin que el administrador de la red tenga que configurar manualmente los túneles, Fig. 3.4.8.2.3.2.

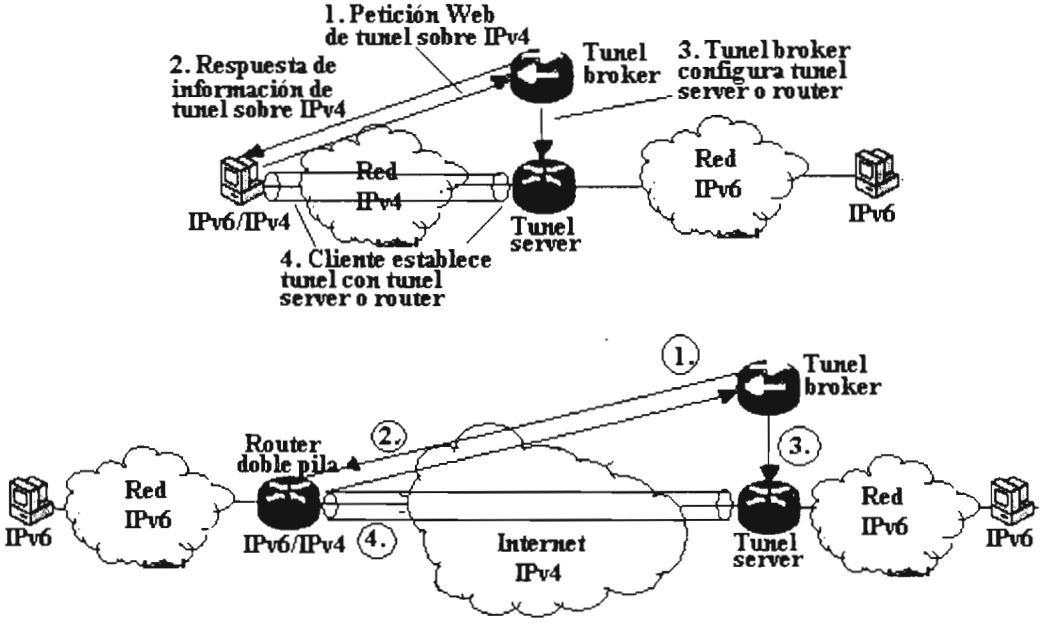


Fig. 3.4.8.2.3.2 Túnel broker o túnel intermediario.

De esta forma, la empresa puede registrar la dirección IPv4 de su sistema final o router remoto mediante el Internet IPv4 con el proveedor de servicios sobre un sitio web dedicado. El proveedor de servicios entrega un script que construye un túnel a la red IPv6, asigna una dirección IPv6 al sistema final y asigna un prefijo de red al router para que permita la conectividad al resto del sitio. El túnel broker administra la creación y delegación del servidor de túneles.
Estos intermediarios permiten que la configuración de estos túneles sea transparente para nosotros con el simple hecho de conocer nuestra dirección IPv4 y sistema operativo, con lo cual algunos nos proporcionan el script que automáticamente configura el túnel.
Algunas de las tareas que el intermediario o proveedor de túneles realiza son: asignación de una dirección IPv6 de su prefijo IPv6 a la maquina a la que se va asignar el túnel, posteriormente, da de alta la maquina en sus registros de DNS y en las tablas de ruteo con lo cual avisa a los demás nodos conectados a este túnel broker que existe un nuevo equipo conectado al 6BONE.
Todo esto se realiza desde la pagina de Internet del tunnel broker. Algunos intermediarios de túneles son:

- 6BONE
- UNAM en la pagina www.ipv6.unam.mx
- Freenet6 en la pagina www.freenet6.net
- WIDE en la pagina 6bone.v6.wide.ad.jp

- CSELT en la pagina carmen.cselt.it/cgi-bin/tb.pl
- Euronet en la pagina www.ipv6.euronet.be
- VBNS en la pagina www.vbns.net

Las nuevas generaciones de túneles brokers son los túnel servers que proporcionan nuevas funcionalidades como:

- Implementación de un protocolo interactivo llamado protocolo de configuración de túnel TSP (Tunnel Setup Protocol).
- El cliente y los servidores pueden intercambiar peticiones y respuestas.
- El cliente puede solicitar: un túnel para un host, un túnel para una red con/sin delegación de prefijo, información de ruteo (RIP, BGP, OSPF), información de nombre de dominio (nombre de host asignado, resolución inversa).

3.4.8.2.4 Túneles automáticos

Los túneles automáticos se configuran, establecen y desaparecen conforme son requeridos, duran tanto tiempo como la comunicación es necesaria.
Cuando un host origen envía un paquete IPv6 a un router IPv6 y el router no puede hacer lo propio tendrá que hacer tunneling. Estos túneles no necesitan configuración manual. Los extremos se determinan automáticamente usando direcciones IPv6 IPv4-compatibles.
Los pasos para realizar el tunneling automático son:

- El datagrama IPv4 que encapsula el trafico IPv6 emplea los 32 bits de orden inferior de las direcciones IPv6 fuente y destino para crear sus equivalentes IPv4 y fija el numero de protocolo a 41 (IPv6).
- La interfaz de red del receptor identifica los paquetes que le llegan como paquetes IPv4 y los pasa a la parte IPv4 de la capa de red dual.
- La capa IPv4 recibe el datagrama del modo normal, reensambla los fragmentos si es necesario, nota que el protocolo es el 41, elimina la cabecera IPv4 y pasa el paquete IPv6 original a la parte IPv6 de la capa de red.
- El código IPv6 procesa el paquete original de la forma habitual. Como la dirección IPv6 de destino del paquete es la dirección IPv6 del nodo (compatible con IPv4) el paquete ha alcanzado su destino. IPv6 procesa cualquier encabezado opcional y pasa el resto de la carga efectiva del paquete al siguiente protocolo listado en la cabecera IPv6.

El tunneling automático lo lleva a cabo un host IPv6/IPv4 que tiene un paquete que enviar a través de un área de tipo IPv4-nativa mediante las siguientes reglas:

- Si el destino es una dirección mapeada a IPv4, envía el paquete usando IPv4 ya que el receptor no soporta IPv6. En otro caso:
- Si el destino se halla en la misma subred, lo envía usando IPv6, ya que el receptor soporta IPv6.
- Si el destino no se halla en la misma subred pero existe un router por default que soporta IPv6 el paquete se le envía a ese router mediante IPv6. En otro caso:
- Si la dirección es compatible con IPv4, el paquete se envía usando tunneling automático.

3.4.8.2.4.1 Túnel Automático compatible-IPv4

El túnel automático compatible-IPv4 es un mecanismo de túnel IPv6 sobre IPv4 que usa una dirección IPv6 compatible-IPv4, es decir inicialmente crear direcciones IPv6 compatibles con IPv4. Recordemos que una dirección IPv6 compatible-IPv4 es la concatenación de ceros en los 96 bits mas a la izquierda y una dirección IPv4 insertada en los últimos 32 bits (esta dirección es la dirección IPv4 asignada al nodo).
Aunque los túneles automáticos se pueden configurar entre sistemas finales, routers de borde, o un router de borde y un sistema final, el túnel automático compatible-IPv4 normalmente se usa para establecer conexión entre routers.
El túnel automático compatible-IPv4 construye túneles con nodos remotos al vuelo, es decir en el momento que se necesiten, no se requiere la configuración manual ya que la fuente y destino del túnel se determinan en base a la dirección IPv4, Fig. 3.4.8.2.4.1.

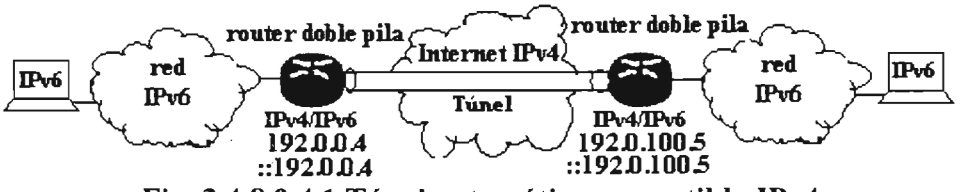


Fig. 3.4.8.2.4.1 Túnel automático compatible-IPv4

Con este mecanismo cuando la interfaz necesita mandar información a la dirección IPv4 de otro nodo, la interfaz automáticamente usa su dirección IPv4 compatible con la cual sabe que tiene que realizar un encapsulamiento dinámico del paquete IPv6 en un datagrama IPv4 cuyo encabezado IPv4 tendrá como dirección fuente los últimos 32 bits de su dirección IPv4 compatible, es decir este mecanismo encapsula paquetes IPv6 en IPv4 y crea los túneles dinámicamente sobre la conexión IPv4 que se tiene.
La desventaja de este mecanismo es que requiere seguir usando direcciones IPv4 por nodo.
Los túneles automáticos compatible-IPv4 son una forma sencilla de crear túneles pero no son buenos para la implementación de redes IPv6, ya que cada host requiere una dirección IPv4, lo que elimina el beneficio del gran espacio de direccionamiento IPv6, por lo que este mecanismo esta siendo desaprobado y reemplazado por el túnel automático 6to4.

3.4.8.2.4.2 Uso de túneles dinámicos 6to4.

El túnel automático y dinámico 6to4, Fig. 3.4.8.2.4.2.1, permite conectar dominios o islas IPv6 sobre una red IPv4 que puede ser el Internet global IPv4 o un backbone corporativo, sin necesidad de tener un túnel estático configurado, estos sitios IPv6 tienen cada uno al menos una conexión a una red IPv4 compartida, también permiten la conexión a redes IPv6 remotas como el 6BONE. Estos túneles son conocidos como dinámicos ya se crean cuando se quiere transmitir la información por Internet IPv4 sin haber configurado ningún dato para el establecimiento de estos.
La técnica 6to4 crea túneles Inter-dominios insertando las direcciones IPv4 como prefijos del sitio IPv6.
El túnel 6to4 ve la infraestructura IPv4 como un enlace sin broadcast virtual, usa una dirección IPv4 insertada en la dirección IPv6 para encontrar el otro extremo del túnel.

Cada dominio IPv6 requiere un router doble pila que automáticamente construye el túnel usando un prefijo de ruteo único 2002::/16 en la dirección IPv6 con la dirección IPv4 concatenada al prefijo de ruteo único, lo que da un prefijo de 48 bits 2002:<Dir. IPv4 ext>::/48, con el identificador de subred se obtiene un prefijo de 64 bits 2002:>Dir. IPv4 ext><Subset ID>::/64. El punto requerido es que cada sitio tenga una dirección IPv6 6to4.

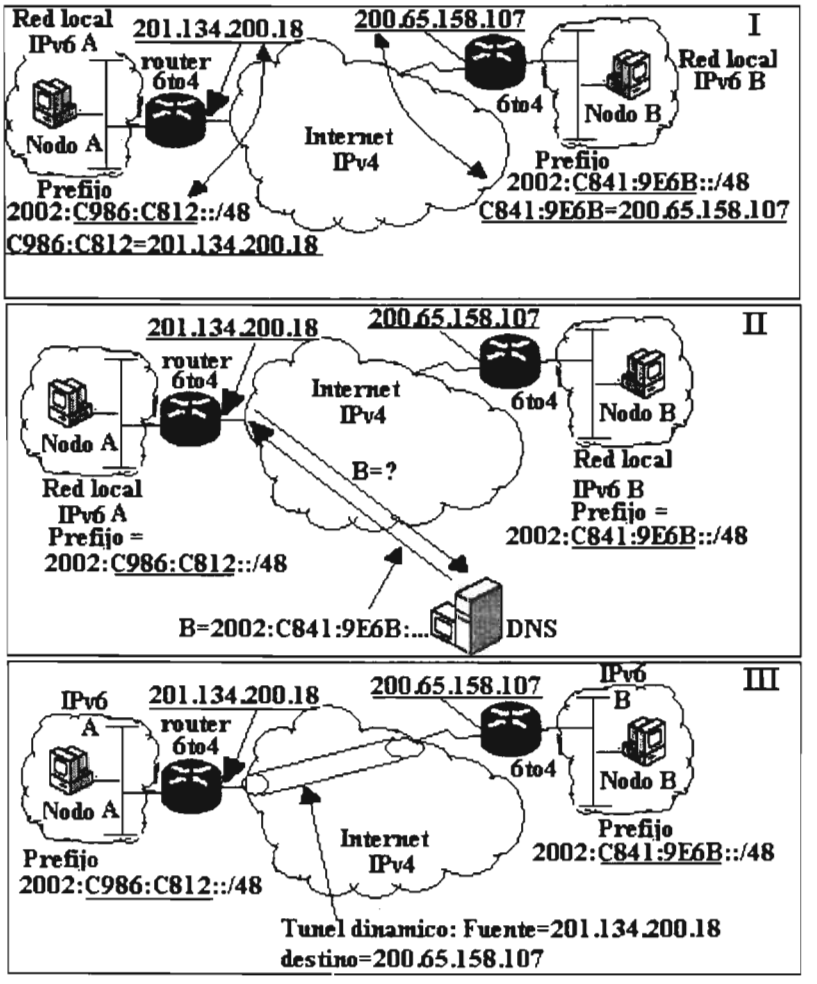


Fig. 3.4.8.2.4.2.1 Mecanismo de túneles dinámicos 6to4 interconectando dominios IPv6

El prefijo 2002::/16 esta asignado para las direcciones de tipo 6to4, un equipo usa este prefijo junto con su dirección IPv4 para construir un prefijo de este tipo 2002:wx:yz::/48, donde los octetos wx y yz estan en forma hexadecimal, cuando el router que posee una dirección 6to4 es requerido a comunicarse a otro sitio, pregunta al servidor DNS la dirección del equipo remoto, cuando se le devuelve la dirección 6to4 del equipo remoto sabe que los campos 2 y 3 después del 2002 son la dirección IPv4 del equipo remoto por lo que usara esa dirección IPv4 y la suya para encapsular dinámicamente los paquetes IPv6.
Lo recomendable es cada sitio tenga solamente una dirección 6to4 asignada a la interfaz externa del router. Además los sitios deberán ejecutar un protocolo de ruteo interior IPv6 como RIPng para el ruteo de IPv6 dentro del sitio, el ruteo exterior es manejado por el protocolo de ruteo exterior IPv4.

Routers relay para la comunicación 6to4.

El uso de routers relay es una etapa que se esta implementando debido a que el uso de IPv6 se esta volviendo mas prevaleciente.

Los routers relay son routers normales o estándar que tienen tanto direcciones IPv6 normales y direcciones IPv6 6to4. Los routers relay 6to4 proporcionan un servicio de ruteo entre el dominio IPv6 nativo (donde funciona un protocolo de ruteo) y el dominio 6to4 (donde no hay un protocolo de ruteo). Por lo menos un router relay se requiere para poder comunicar sitios 6to4 y dominios IPv6 nativos, Fig. 3.4.8.2.4.2.2, ya que la técnica 6to4 permite al router de borde de la red enviar paquetes a cualquier destino con prefijo 2002::/16, pero cualquier otro sitio IPv6 que no tenga este prefijo será inalcanzable a menos que uno de los routers 6to4 de núcleo funcione como router relay 6to4 y permita reenviar trafico al Internet IPv6.

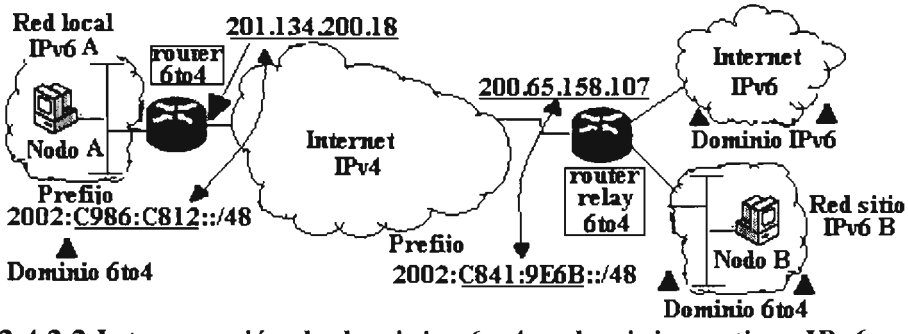


Fig. 3.4.8.2.4.2.2 Interconexión de dominios 6to4 y dominios nativos IPv6 mediante un router relay 6to4

Los routers 6to4 manejan un protocolo de ruteo interior IPv6 para el ruteo IPv6 dentro del sitio, pero participan en el ruteo interdominio IPv6 usando una ruta IPv6 por default que apunta a un router relay especifico.

3.4.8.2.4.3 Túneles ISATAP

Los túneles ISATAP (Intrasite Automatic Tunneling Addressing Protocol-Protocolo de direccionamiento mediante túneles automáticos intrasitio) son un mecanismo parecido a los túneles 6to4 ya que permiten la instalación de IPv6 usando la infraestructura IPv4 como una capa de acceso multiacceso sin broadcast NBMA (Non Broadcast Multiaccess).

El mecanismo de transición ISATAP permite la instalación de IPv6 para nodos de forma simple y a gran escala dentro de la red IPv4 existente de un sitio sin preocuparse de temas de agregación o escalabilidad y sin que se necesiten instalar servicios IPv4 especiales como multicast.

Todos los nodos ISATAP manejan la de doble pila de protocolos IPv4 e IPv6. Los túneles ISATAP se pueden usar sobre redes de campus o en la transición de sitios locales. El mecanismo ISATAP soporta el ruteo IPv6 dentro de dominios de ruteo IPv6 globales y de sitio-local, maneja túneles IPv6 a través de porciones de una red IPv4 de un sitio sin algún soporte IPv6 nativo, también soporta túneles automáticos dentro de sitios que usan asignaciones de dirección IPv4 no globalmente únicas combinadas con la traducción de direcciones de red NAT. La Fig. 3.4.8.2.4.3.1 muestra un esquema de tunelización ISATAP.

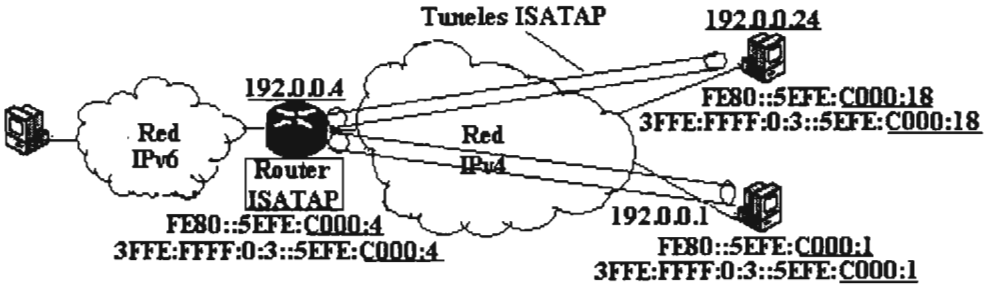


Fig. 3.4.8.2.4.3.1 Túneles ISATAP

Las direcciones ISATAP se forman con un prefijo de red de 64 bits y el identificador de interfaz de 64 bits se forma concatenando los campos 0000:5EFE y la dirección IPv4 del nodo de doble pila, así las direcciones FE80::5EFE:10.0.1.1, FEC0::5EFE:192.0.0.4, 3FFE:FFFF:0:3:0:5EFE:192.0.100.50 son direcciones ISATAP.
La tunelización ISATAP normalmente se realiza únicamente dentro de los limites de un sitio, por lo que la dirección IPv4 no necesita ser globalmente única.
El mecanismo ISATAP así como el 6to4 proporcionan conectividad IPv6 a un nodo bajo tres escenarios típicos: un ISP o red empresarial que proporciona conectividad IPv6, el nodo tiene acceso a por lo menos una dirección IPv4 global o la red empresarial ha instalado un router ISATAP.

3.4.8.2.4.4 Túneles Teredo

Teredo es también conocido como un traductor de dirección de red IPv4 transversal para IPv6.
El mecanismo de túneles Teredo (shipworm-gusano de transporte) es una tecnología de transición que proporciona asignación de dirección y tunelización automática de host a host para la conectividad unicast IPv6 a los nodos localizados detrás de uno o más dispositivos NAT IPv4, para lo cual tuneliza paquetes IPv6 sobre el protocolo de transporte UDP a través de dispositivos NAT. El servicio Teredo es usado para el caso cuando el dispositivo NAT no puede ser actualizado para manejar ruteo IPv6 nativo o actuar como un router 6to4.
Los paquetes IPv6 encapsulados en IPv4 son mandados con el campo de protocolo del encabezado IPv4 puesto a 41. Muchos dispositivos NAT solo traducen trafico TCP o UDP y deben manualmente ser configurados para traducir otros protocolos, por lo que el trafico IPv6 encapsulado no fluirá a través de dispositivos NAT típicos. Para permitir que el trafico IPv6 fluya a través de dispositivos NAT el paquete IPv6 es encapsulado como un mensaje UDP IPv4 conteniendo un encabezado IPv4 y encabezado UDP. Los mensajes UDP pueden ser traducidos universalmente por dispositivos NAT.
Por lo tanto la tecnología Teredo permite el uso de túneles automáticos IPv6 entre hosts que están localizados a través de uno o más dispositivos NAT, por que el trafico de los hosts Teredo es mandado como un mensaje UDP IPv4. Si el dispositivo NAT soporta la traducción de puestos UDP entonces soporta Teredo.
Los túneles teredo usan servidores teredo y relevadores (relays) Teredo, Fig. 3.4.8.2.4.4.1.

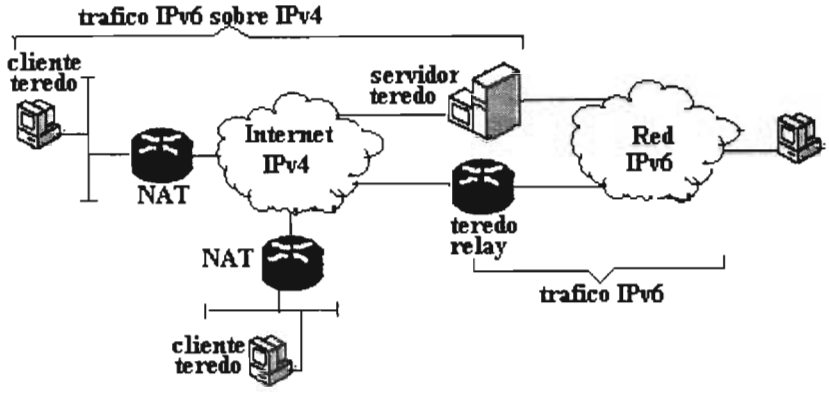


Fig. 3.4.8.2.4.4.1 Infraestructura teredo

Los servidores Teredo usan una autoconfiguración del tipo stateless y administran una pequeña fracción del trafico entre clientes Teredo, los relay Teredo funcionan como routers IPv6 entre el servicio Teredo y el Internet IPv6 nativo. De esta forma una red Teredo consiste de un conjunto de clientes Teredo que no requieren configuración a los cuales se asigna un prefijo de dirección IPv6 especialmente formado, servidores Teredo y relays Teredo, estos dos últimos usan direcciones IPv4 globalmente únicas.

La siguiente tabla resume algunas características del mecanismo de túneles:

Tipo de túnel	Uso	Limitaciones	Requerimientos
Túnel IPv6 manual	Enlaces seguros y estables para la comunicación normal	Túnel entre dos puntos únicamente, gran sobreencabezado de administración	Dirección IPv6 registrada del ISP. Routers doble pila
Túnel IPv6 sobre GRE IPv4	Enlaces seguros y estables para la comunicación normal	Túnel punto-punto, gran sobreencabezado de administración. No permite la conexión al 6BONE	Dirección IPv6 registrada del ISP. Routers doble pila
Tunel Broker	Sistemas IPv6 aislados	Seguridad	Configuración y admón.. de túnel por ISP. Conocimientos de como crear y mandar scripts para los diferentes equipos
Túnel automático compatible con IPv4	Sitios pequeños o para un solo usuario con comunicación poco frecuente	Comunicación solamente con otros sitios IPv4-conpatible	Prefijo IPv6 ::/96. Router doble pila.
Túnel automático 6to4	Comunicación de varios dominios IPv6 remotos. Comunicación		Prefijo IPv6 2002::/16. Router doble pila. Fácil de configurar sin sobreencabezado de

	frecuente		administración.
Túneles ISATAP	Transición de sitios no ruteados	No disponible comercialmente	Router doble pila.
Túneles 6over4	Transición de sitios no ruteados		

Estos dos mecanismos de doble pila y túneles (dual stack y tunneling) se diseñaron para que se usen por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y para que utilicen las infraestructuras de ruteo IPv4. Muchos nodos necesitaran compatibilidad por mucho tiempo y quizás indefinidamente. Sin embargo algunos nodos puede que no necesiten usar ni implementar estos mecanismos, ya que puede ser que trabajen en ambientes donde no requieran interoperabilidad con IPv4.

3.4.8.3 Implementación de IPv6 sobre enlaces de datos dedicados.

Se pueden usar las tecnologías de capa 2 (Frame relay, ATM, ópticas DWDM) para conectar los routers de la red a las WAN o MAN de algún ISP, estos routers tendrán una configuración que permita usar la misma infraestructura de capa 2 para IPv4 pero funcionando con IPv6 sobre ATM, circuitos virtuales permanentes PVCs o enlaces ópticos separados, Fig. 3.4.8.3.1.

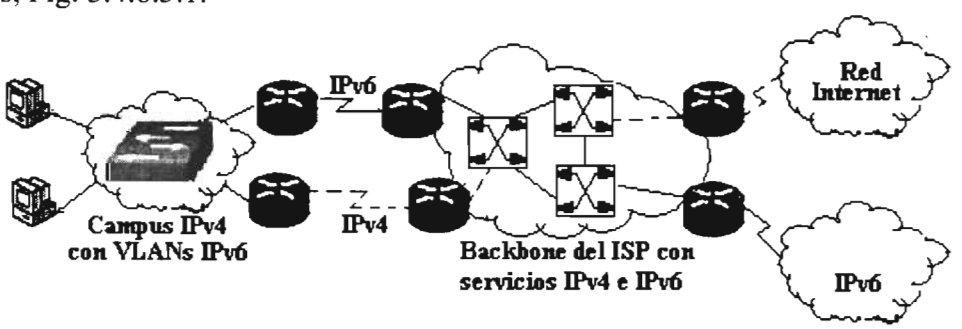


Fig. 3.4.8.3.1 Ejemplo de un esquema para IPv6 sobre enlaces de datos dedicados.

Con esta configuración el ISP no tendrá perdidas en ingresos o servicios IPv4.

3.4.8.4 Implementación de IPv6 sobre backbones MPLS

La instalación de IPv6 sobre backbones de conmutación de etiquetas multiprotocolo MPLS (Multiprotocol Label Switching) permite que los dominios aislados de IPv6 con otros sobre el núcleo de una red IPv4 MPLS. Con una configuración de este tipo se requiere menos actualización de la infraestructura del backbone y menos reconfiguración de los routers del núcleo, puesto que el reenvío se basa en etiquetas mas que en el encabezado IP, lo que permite una estrategia de costos muy efectiva para la instalación de IPv6.
Los servicios de ingeniería de trafico y VPNs disponibles en un ambiente MPLS permiten que las redes IPv6 se combinen en VPNS o extranets sobre una infraestructura que soporta VPNs IPv4 y MPLS-TE. Algunas estrategias de implementación son:

- Instalación de IPv6 mediante túneles sobre los routers de borde del cliente (CE). Esta estrategia no requiere cambios en los routers P o PE del proveedor MPLS, gracias a que encapsula el trafico IPv6 en túneles IPv4, con lo que el trafico IPv6 aparenta ser trafico IPv4.
- Instalación de IPv6 sobre un circuito de transporte sobre MPLS. Esta estrategia solamente se aplica a routers Cisco y no requiere cambios a los mecanismos de ruteo del núcleo.
- Instalación de IPv6 sobre los routers de borde del proveedor (PE) también llamados 6PE. Esta implementación requiere cambios en los routers PE para manejar la doble pila, todas las funciones del núcleo permanecen trabajando con IPv4.
- Otra estrategia podría ser tener un núcleo MPLS de IPv6 nativo, pero esta estrategia requiere una actualización de red completa a todos los routers P y PE con doble control tanto para IPv4 e IPv6.

- **Instalación de IPv6 mediante túneles sobre los routers de borde del cliente (CE)**

El uso de túneles en los routers de borde del cliente CE (Customer Edge), Fig. 3.4.8.4.1, es la forma más simple de instalar IPv6 sobre redes MPLS, ya que no impacta la operación de la infraestructura MPLS además de que no requiere cambios a los routers P del núcleo o a los routers PE (Provider Edge) conectados a los clientes.

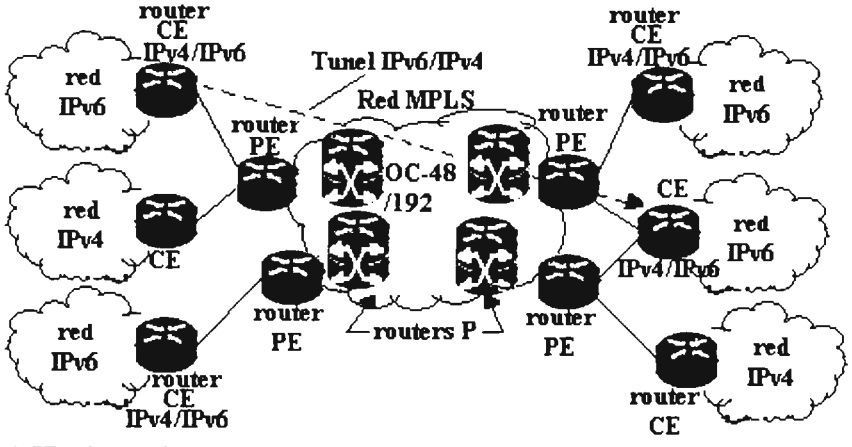


Fig. 3.4.8.4.1 IPv6 mediante túneles en los routers CE para funcionamiento sobre un backbone MPLS.

En este caso la interconexión de dominios IPv6 mediante los túneles sobre IPv4 es similar a las VPNs MPLS que soportan túneles IPv4 nativo.
Los routers CE deben soportar ambas pilas IPv4 e IPv6 y deberán ser configurados para soportar túneles manualmente configurados o 6to4, pero la comunicación con los routers de proveedor PE es mediante IPv4, con lo que el trafico para el dominio MPLS se presenta como IPV4. Los routers CE de doble pila usan direcciones 6to4 o un prefijo IPv6 asignado por un proveedor.

- Instalación de IPv6 sobre un circuito de transporte sobre MPLS

Esta estrategia usa cualquier circuito de transporte para implementar IPv6 sobre redes MPLS, lo cual no impacta la operación de la infraestructura MPLS, además de que no

requiere cambios en los routers P del núcleo y tampoco en los routers PE conectados al cliente. La conexión entre sitios remotos ejecuta el protocolo IPv6 nativo sobre enlaces dedicados, donde los mecanismos subyacentes son transparentes a IPv6, Fig. 3.4.8.4.2.

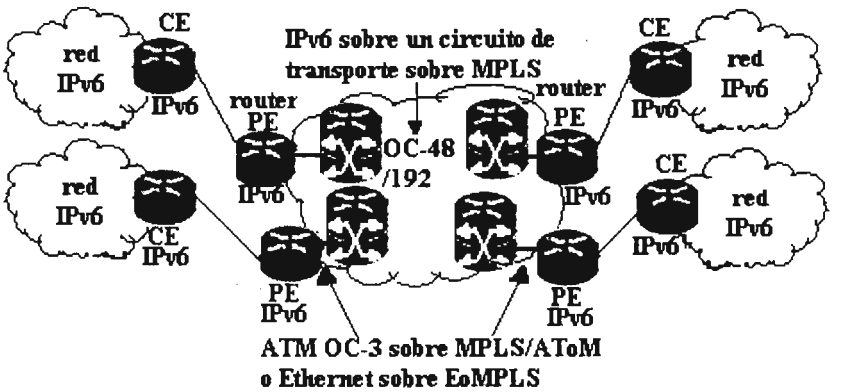


Fig. 3.4.8.4.2. IPv6 sobre un circuito de transporte sobre MPLS

El trafico IPv6 es encapsulado usando cualquier transporte sobre MPLS como ATM sobre MPLS (AToM) o ethernet sobre MPLS (EoMPLS), los routers se conectan a través de un OC-3 de ATM o una interfaz ethernet.

- Instalación de IPv6 sobre los routers de borde del proveedor 6PE.

Esta estrategia configura IPv6 sobre los routers PE MPLS, con lo que el proveedor de servicios no necesita actualizar ni el hardware ni el software del núcleo de red, por lo que los ingresos de trafico IPv4 no serán afectados.
Esta implementación mantiene intactas las características actuales de MPLS como servicios MPLS o VPN para IPv4, además de que simula proporcionar un servicio nativo IPv6 para los clientes empresariales (para lo cual el ISP proporcionara prefijos IPv6), también soporta VPNs IPv6.
En este esquema el envío es realizado por conmutación de etiquetas, con lo que no es necesario usar túneles IPv6 sobre IPv4 o encapsulamiento de capa 2, lo que simula ser un servicio de IPv6 nativo a través de la red, Fig. 3.4.8.4.3.
Los routers 6PE deben ser actualizados para soportar las dos pilas de protocolos IPv4 e IPv6 y sus interfaces conectadas al núcleo deben manejar MPLS. Según las necesidades que se tengan cada router puede ser configurado para enviar trafico IPv6 o IPv4 en las interfaces conectadas a los routers CE, así pueden ofrecer IPv6 nativo o ambos servicios IPv6 e IPv4 nativos. El router 6PE intercambia información de ruteo ya sea IPv4 o IPv6 a través de los protocolos de ruteo soportados según el tipo de conexión y switchea el trafico IPv4 e IPv6 sobre las interfaces nativas IPv4 e IPv6 que no ejecutan MPLS.
El intercambio de información de alcanzabilidad entre routers 6PE en el dominio MPLS se realiza con BGP multiprotocolo y comparten un protocolo de ruteo común IPv4 como OSPF e IS-IS con otros dispositivos P y PE en el dominio.

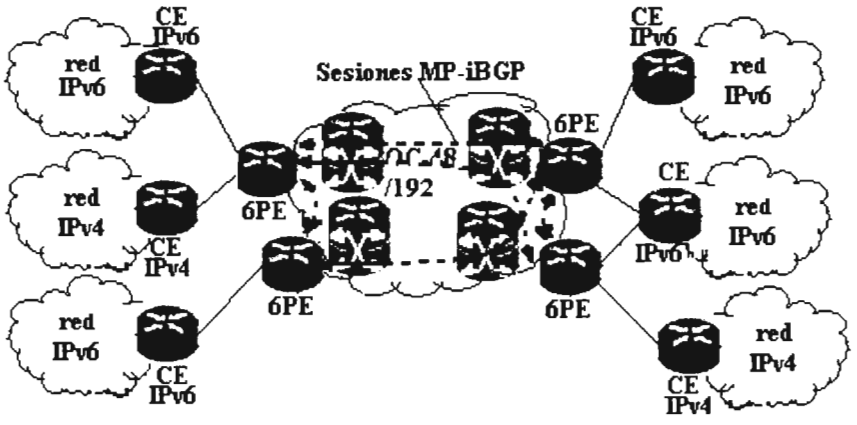


Fig. 3.4.8.4.3 Instalación de IPv6 en los routers 6PE

El encapsulamiento del trafico IPv6 en los routers 6PE se realiza mediante dos niveles de etiquetas MPLS. La etiqueta superior se distribuye mediante un protocolo de distribución de etiqueta LDP (Label Distribution Protocol) o TDP (Tag Distribution Protocol), este protocolo es usado por los dispositivos en el núcleo para transportar el paquete destinado a un destino 6PE usando información de ruteo IPv4. La segunda etiqueta o etiqueta inferior se asocia con el prefijo IPv6 del destino a través del multiprotocolo BGP-4.
La siguiente tabla resume las características de la implementación de IPv6 sobre backbones MPLS.

Mecanismo MPLS	Uso	Beneficios	Limitaciones	Requisitos
IPv6 usando tuneles sobre los routers CE	Clientes que desean usar IPv6 sobre los servicios MPLS existentes	No impacta a infraestructura MPLS	Los routers usan direcciones compatible-IPv4 o 6to4	Router CE doble pila
IPv6 sobre un circuit de transporte sobre MPLS	ISPs con enlaces ATM o Ethernet a los routers CE	Comunicación IPv6 totalmente transparente	Los tráficos IPv4 e IPv6 no se mezclan	Modelos especifico de routers en el nucleo.
IPv6 sobre router PE	Proveedores de servicios móviles y de Internet que quieren ofrecer un servicio IPv6	Actualización de los routers PE de bajo costo y bajo riesgo, no impacta al núcleo MPLS	No soporta FVPN	Actualización de software IPv6 a router PE

La segunda fase de la migración a IPv6 consiste en implementar una infraestructura de IPv6-nativo, dicha fase solamente deberá ser completada cuando ya no sea necesaria la interoperabilidad con IPv4. Esta fase es más delicada debido al esfuerzo que implica la planificación e instalación de los routers que traducirán las cabeceras adecuadas para que los nodos IPv6 interoperen con nodos IPv4.

3.4.8.5 Traducción de cabeceras

Las estrategias de migración anteriormente mencionadas permiten implementar IPv6 de extremo a extremo. Puede haber organizaciones que no deseen implementar dichas estrategias, o pueden instalar una red IPv6 pura sin soporte de las dos pilas, o en caso de que soporten las dos pilas puede que no posean direcciones IPv4.
Bajo estas situaciones se requiere poder intercomunicar hosts IPv6-nativos con hosts IPv4-nativos, para poder realizar esto se debe poder implementar algún nivel de traducción entre los protocolos IPv4 e IPv6 en un host, en un router o en hosts de doble pila. El host debe poder entender cual protocolo usar, ya que por ejemplo una red IPv6-nativa puede querer ser capaz de acceder a los recursos IPv4-nativos, como servidores web IPv4-nativo.
Los nodos solo IPv6 requieren traducir cabeceras cuando establecen comunicación con nodos solo IPv4, esta parte opcional del SIT la implementan los routers IPv6/IPv4 situados en las fronteras entre áreas IPv6-complete e IPv4-complete. El trafico puede ser IPv4 o IPv6.
El trafico IPv4 es el trafico de un área IPv4-complete que entra en un área IPv6-complete.
El trafico IPv6 es el trafico de un área IPv6-complete que entra en un área IPv4-complete.
Estos tipos de trafico pueden ser terminales (cuando van dirigidos a un nodo dentro del área) o transitorios (cuando se dirigen a un nodo fuera del área).
Los routers traductores tiene que seleccionar la forma adecuada de las direcciones IP, además de mapear correctamente las direcciones a traducir:

- Las direcciones IPv4 se obtienen tomado los 32 bits de orden inferior de la dirección IP. Si la fuente o el destino son solo IPv6, la cabecera es intraducible.
- Las direcciones fuente IPv6 se crean añadiendo el prefijo de 96 bits 0:0:0:0:0:0 a la dirección IPv4.
- Las direcciones destino IPv6 se crean agregando el prefijo de 96 bits 0:0:0:0:0:ffff a la dirección IPv4 para generar una dirección IPv6 compatible con IPv4 para el trafico terminal o el prefijo de 96 bits 0:0:0:0:0:0 para una dirección IPv6 mapeada a IPv4 para el trafico de transito.

La traducción IPv4-IPv6 es una extensión de las técnicas de traducción NAT, usadas para traducir el formato del encabezado así como también las direcciones.
Algunos mecanismos de traducción de IPv6 a IPv4 son:

- Traducción de protocolo-traducción de dirección de red (NAT-PT).
- Conmutación TCP-UDP.
- Bump in the Stack (BIS).
- Mecanismo de transición de doble pila (DSTM).
- Gateway basado en SOCKS.

Estos mecanismos son más importantes conforme IPv6 es el protocolo por default y que permite a los sistemas IPv4 ser parte de la red IPv6.
Los mecanismos BIS y NAT-PT que permiten la comunicación entre hosts IPv6-nativo y hosts IPV4-nativo usan el algoritmo SIIT (Stateless IP/ICMP Translator), el cual realiza su función de traducción paquete-por-paquete de los encabezados IP entre IPv4 e IPv6 y traduce las direcciones entre IPv4 y ya sea direcciones IPv6 IPv4-traducidas o direcciones IPv6 mapeadas-IPv4.

3.4.8.5.1 Traducción de protocolo-traducción de dirección de red (NAT-PT).

La traducción de protocolo y de dirección de red NAT-PT (Network Address Translation-Protocol Translation) permitirá a los ISPs con IPv6-nativo interconectarse con los hosts y aplicaciones IPv4, este mecanismo será muy importante cuando la mayor parte de la infraestructura de Internet sea IPv6.
Este mecanismo traduce en la capa de red las direcciones IPv4 e IPv6 y permite que las aplicaciones IPv6 se comuniquen con hosts y aplicaciones IPv4 nativos.
Un gateway de nivel de aplicación ALG (Aplication Level Gateway) realiza la traducción entre las peticiones y respuestas DNS IPv4 e IPv6.
NAT-PT tiene las mismas limitaciones de NAT IPv4, además de ser un punto de falla, el pobre desempeño de un ALG mas las limitaciones de los tipos de aplicaciones que soporta disminuyen el valor y utilidad de la red, aunque permite la seguridad a nivel aplicación no permite la implementación de la seguridad en la capa IP de extremo a extremo, hace la fusión de las redes con direccionamiento privado muy difícil.

3.4.8.5.2 Conmutación TCP-UDP.

Este mecanismo es similar a NAT-PT ya que requiere un servidor dedicado y DNS, este mecanismo realiza la traducción en la capa de transporte, el DNS proporciona el mapeo entre direcciones IPv4 e IPv6.
Cuando el servidor relay TCP recibe una petición, establece conexiones separadas en el nivel de transporte para ambos hosts fuente y destino IPv4 e IPv6, y transfiere los datos de una conexión a la otra. El relay UDP trabaja en forma similar.
Es muy usado para accesar hosts IPv4-nativos (servidores web IPv4) sin tener que actualizar el lado IPv4 o IPv6. Soporta trafico bidireccional, permite la seguridad a nivel aplicación pero no a nivel de red, el reenrutamiento rápido es difícil.

3.4.8.5.3 Bump in the stack.

El mecanismo BIS (Bump in the stack) que es parte del SIIT se usa para la comunicación entre aplicaciones IPv4 sobre hosts IPv4-nativos y hosts IPv6-nativos, para ello se agregan tres capas al stack del protocolo IPv4 (extensión de resolución de nombre, mapeador de dirección y traductor de dirección) para que cuando una aplicación requiera comunicarse con un host IPv6-nativo las capas adicionales se encargan de mapear la dirección IPv6 en la dirección IPv4 del host IPv4. Este mecanismo se aplica solamente a sistemas finales y mediante una extensión puede ser usado por hosts de doble pila.

3.4.8.5.4 Mecanismo de transición de doble pila (DSTM).

El mecanismo de traducción de doble pila DSTM (Double Stack Translation Mechanism) se aplica en hosts de doble pila que no tienen una dirección IPv4, pero necesitan comunicarse sistemas IPv4. Se requiere un servidor dedicado que dinámicamente proporciona una dirección IPv4 global temporal, obtenida mediante DHCPv6 (esta dirección es asignada por el tiempo que dure la comunicación), también usa túneles

dinámicos para transportar el trafico IPv4 dentro de un paquete IPv6 a través del dominio IPv6.
Este mecanismo será muy importante conforme el uso de IPv6 sea mayor aunado al crecimiento en la escasez de direcciones IPv4, las cuales probablemente deberán ser compartidas entres hosts, asimismo será importante en el caso de que se requiera transportar trafico IPv4 sobre IPv6 así como para comunicar los hosts IPv6 que se encuentran en un dominio IPv6 con sistemas remotos IPv4 legados.

3.4.8.5.5 Gateway basado en SOCKS.

El mecanismo del gateway IPv6/IPv4 basado en socks permite la comunicación entre hosts IPv4-nativo e IPv6-nativo, este agrega funcionalidad a los sistemas finales (cliente) y gateways para poder implementar un ambiente en el que se pueda switchear dos conexiones terminadas IPv4 e IPv6 en la capa de aplicación. El mecanismo se basa en el protocolo SOCKSv5 y usa una característica llamada delegación de resolución de nombres DNS para determinar las direcciones IPv6, delegando la resolución de nombre al gateway, por lo que no requiere cambios en el DNS existente.
Estos mecanismos de traducción de protocolo además de permitir la instalación de IPv6 dentro del ambiente IPv4 permiten la comunicación entre aplicaciones que usan IPv4 y aplicaciones que usan IPv6, como es el caso de los navegadores web IPv6-nativos que necesitan comunicarse con servidores web IPv4-nativos. Dichos mecanismos son útiles para pasar de la fase de prueba a la de uso, además permitirán a los sistemas heredados IPv4 ser parte de la red IPv6 completa. Estos mecanismos permitirán la traducción entre los protocolos IPv4 e IPv6 sobre sistemas finales, servidores dedicados y routers que se encuentran en la red IPv6 y sumados a los hosts de doble pila permitirán un conjunto completo de herramientas para la instalación de IPv6 sin interrumpir el trafico IPv6.
Puede ser preferido el uso de la traducción de protocolo IPv4-IPv6 para el funcionamiento de nuevos dispositivos de Internet como celulares, carros o electrodomésticos.
La siguiente tabla resume algunas características de los mecanismos de traducción de protocolo:

Mecanismos de traducción	Uso	Beneficios	Limitaciones	Requisitos
NAT-PT	Hosts IPv6-nativo a hosts IPv4-nativo	No usa doble pila	No existe seguridad end-to-end. Servidor dedicado=punto de falla	Servidor dedicado. DNS con soporte IPv6
TCP-UDP Relay	Traducción entre IPv6 e IPv4 sobre un servidor dedicado		No existe seguridad end-to-end. Servidor dedicado=punto de falla	Servidor dedicado. DNS con soporte IPv6
BIS	Comunicación entre hosts IPv4-nativo y hosts IPv6-nativo	Implementación en sistemas finales	Todas las pilas deben ser actualizadas	Pila IPv4 actualizada

DSTM	Hosts de doble pila	Asignación IPv4 temporal asignada de un grupo		Servidor dedicado asigna la dirección IPv4 temporal global.
SOCKS	Hosts IPv6-nativo a hosts IPv4-nativo		Software adicional en el router	Software cliente y gateway en el cliente y router

La siguiente tabla resume algunos datos de las estrategias:

Estrategia	Uso primario	Beneficios	Limitaciones	Requisitos
IPv6 sobre túneles IPv4	El ISP quiere ofrecer un servicio IPv6 inicial. La empresa quiere interconectar dominios IPv6 o enlazarse a redes IPv6 remotas.	Demanda de IPv6 con mínima inversión. Fácil de implementar sobre la infraestructura IPv4. Bajo costo, bajo riesgo.	Diagnostico y administración complejos por la independencia del túnel y topología de enlace.	Acceso a IPv4 a través de un router de doble pila. Acceso a DNS IPv6.
IPv6 sobre enlaces de datos dedicados	WAN´s MAN´s del ISP implementando ATM, Frame Relay o DWDM.	Proporciona IPv6 de extremo a extremo sin impacto en el trafico IPv4	Falta de hardware especifico IPv6 para el soporte y administración de IPv6 en el hardware actualmente instalado	Acceso a la WAN a través de un router de doble pila. Acceso a DNS IPv6.
IPv6 sobre backbones MPLS	Los proveedores de servicio móvil o regional implementan MPLS	Integra IPv6 sobre MPLS, por lo que el hardware y software del núcleo no necesita ser actualizado	Implementación requerida de MPLS. Mucho sobreencabezado de administración	Cambios mínimos en los routers de borde del cliente (CE) o del proveedor (PE), dependiendo de la técnica
Uso de backbone doble pila	Pequeñas redes empresariales	Fácil de implementar en redes pequeñas con mezcla de aplicaciones IPv4 e IPv6.	Administración doble de protocolos de ruteo	Routers doble pila. Acceso a DNS IPv6. Mas memoria, 2 tablas de ruteo IPv4 e IPv6.

Consideraciones generales para la implementación de IPv6

Para realizar la transición hacia IPv6, los fabricantes lideres en el tema recomiendan que la transición empiece desde los bordes de la red para posteriormente continuar hacia el núcleo, de manera que se maneje un buen control de los costos, no se interrumpa el servicio de IPv4 y el esfuerzo dedicado a dicha transición se enfoque a las necesidades de as aplicaciones.

- **Consideraciones generales para la implementación de IPv6 en un ambiente de un ISP.**

En un ambiente de un proveedor de servicios de Internet la implementación podría realizarse en las siguientes tres fases:

- Instalación del servicio IPv6 a nivel de acceso del cliente.
  Instalando el servicio IPv6 en el punto de acceso del cliente, toda la infraestructura fuerte que compone al núcleo se mantiene intacta en esta etapa, además que los servicios con IPv4 que ofrece dicha infraestructura continúan ofreciéndose. Con esta implementación inicial se pueden evaluar productos y servicios IPv6, al mismo tiempo que se puede realizar una valoración de la demanda de iPv6 sin una inversión mayor.
- Implementación de IPv6 en la infraestructura del núcleo.
  En esta fase se pueden actualizar los routers del núcleo de la red para que soporten tanto IPv4 como IPv6, o se puede continuar haciendo los routers IPv6-nativos para que manejen solamente IPv6 conforme el trafico IPv6 se vuelva predominante.
- Interconexión con otros proveedores de servicios IPv6.
  En la tercera fase ya se pueden realizar conexiones con otros ISPs o con la red de pruebas de IPv6 6BONE lo que además de permitir evaluar IPv6 ayudara a comprender mejor los requerimientos necesarios para la comunicación con IPv6.

- **Consideraciones generales para la implementación de IPv6 en un ambiente de red empresarial.**

La implementación de IPv6 en la red de una empresa puede realizarse para probar las aplicaciones IPv6 que pudieran usarse en la red, de esta forma se pueden evaluar el direccionamiento de extremo a extremo, la autoconfiguración, la calidad de servicio de extremo a extremo, la seguridad de extremo a extremo, o se puede expandir el esquema de direccionamiento que permitan el manejo y despliegue de nuevo servicios como el del sistema telefónico basado en IP. Para probar y evaluar los productos y servicios IPv6 en forma general se recomiendan los siguientes dos esquemas:

- Configurar un dominio IPv6 y conectarlo a una red IPv6 remota existente como la red IPv6 de pruebas 6BONE.
- Configurar dos o más dominios IPv6 e interconectarlos sobre la infraestructura IPv4 existente.

Las características de IPv6 están diseñadas para simplificar la migración, ya que las direcciones IPv6 se pueden derivar de las direcciones IPv4, los túneles IPv6 se pueden construir sobre las redes IPv4, los nodos IPv6 seguirán el enfoque de doble pila para el soporte de IPv4 e IPv6 al mismo tiempo.

4. RED LAN PROPUESTA PARA LA MIGRACIÓN TECNOLÓGICA A IPV6

4.1 Topología de red actual

La red LAN que se propone para realizar la actualización tecnológica para el manejo de protocolo IPv6 es mostrada en la Fig. 4.1.1

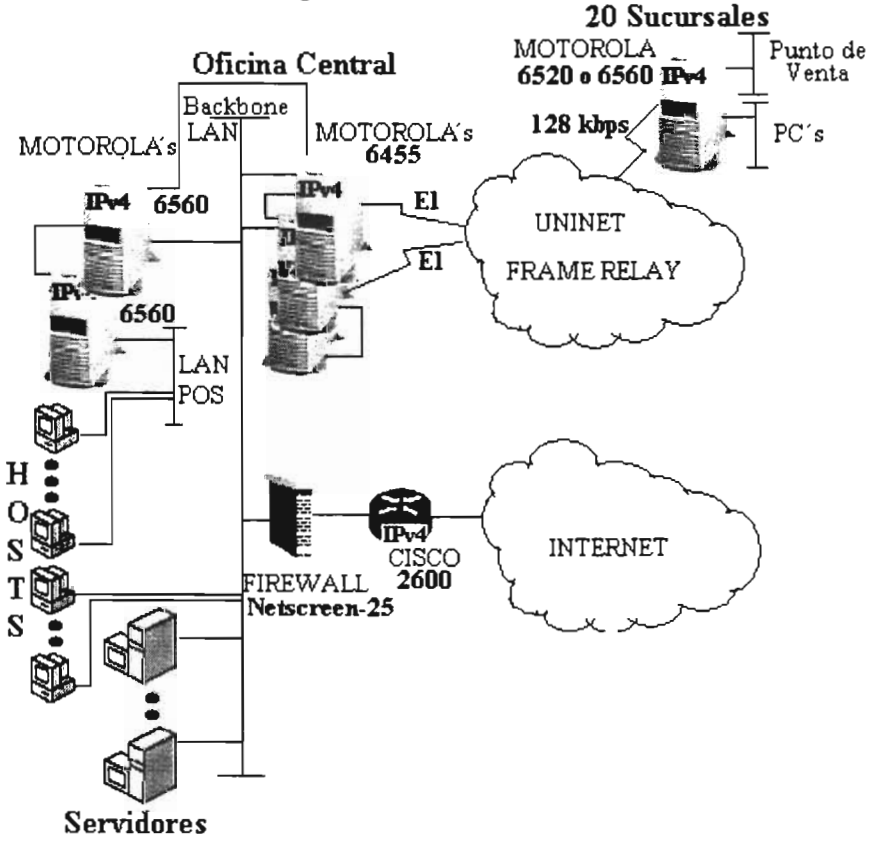


Fig.4.1.1 Esquema de la red Lan que se desea actualizar de IPv4 a IPv6

La red LAN propuesta es parte de una red de comunicaciones compuesta de un nodo central y 20 sucursales.

Todas las sucursales se conectan a la oficina central a través de enlaces WAN Frame Relay de 128 kbps de CIR., estos enlaces son recibidos en la oficina central a través de 2 E1 que balancean la carga de sucursales recibidas en cada uno de ellos. Los E1 se reciben en equipos Motorola, los cuales manejan tanto la voz como los datos encapsulados en Frame Relay para la comunicación entre oficina central y sucursales.

Al segmento LAN de la oficina central se conecta un equipo Cisco 2600 que da salida a Internet mediante un enlace WAN PPP dedicado de 2 Mbps.

La red LAN sobre la que se enfoca nuestra atención es la de la oficina central.

La plataforma de ruteo de la red es de la marca Motorola. En la oficina central se tiene un cluster de 4 routers marca Motorola (modelos 6560 y 6455) interconectados entre si. Un router sirve como puerta de enlace de la subred de punto de venta y otro es la puerta de enlace de las dos subredes usadas para los hosts y servidores, estas dos subredes las maneja

el mismo router por medio de direcciones IP en subinterfaces, este mismo router retransmite el trafico que va dirigido hacia Internet por medio del equipo firewall y posteriormente por el ruteador Cisco.
Del cluster de routers que se tienen en la oficina central dos de ellos son los que reciben los enlaces frame relay que conectan a las sucursales.
En la oficina central se tienen 3 segmentos de red diferentes que componen la red LAN:

- Se tiene una red LAN Ethernet para punto de venta con direccionamiento clase C igual a 192.0.254.0.
- Dos redes para el direccionamiento usado para los hosts en general, servidores y ruteadores, las dos subredes son clase C 192.0.0.0 y 192.0.100.0.

Se tiene una conexión WAN hacia Internet por medio de un enlace dedicado de 2 Mbps con UNINET, en este enlace el protocolo de capa de enlace usado es el protocolo PPP, antes de salir a Internet se tiene que pasar por un firewall de la marca Netscreen.
El enlace de Internet se recibe directamente en el ruteador Cisco modelo 2600 con versión de IOS 12.1(2)T, desde este equipo se levanta el protocolo PPP con el ISP UNINET.
EL ISP junto con el enlace proporciona un pool de 10 direcciones publicas homologadas IPv4. El router Cisco hace la traducción de direcciones NAT (Network Address Translation) de la red interna al conjunto de direcciones publicas homologadas.
En la misma oficina central se encuentran hospedados los servidores de la Intranet, antivirus, correo, HP-9000 y Tandem.
El servidor que contiene la pagina Web de la empresa y el de correo se encuentran hospedados con un proveedor de servicio de hosting.
Los sistemas operativos de la mayoría de los servidores son Microsoft Windows NT, un Linux, Unix para la HP-9000 y Base24 para la Tandem.
Todas las PCs y laptops de los usuarios son de la marca Compaq con sistema operativo Microsoft Windows XP.
En cada una de las sucursales se tienen a su vez también dos redes Ethernet una para punto de venta y otra para el centro de computo conectadas al router de la sucursal por medio de dos tarjetas de red ethernet, una para la subred de punto de venta y la otra para la subred de PCs y servidores.
En cada sucursal se tiene un servidor HP-9000 que maneja las aplicaciones de las diferentes áreas y un servidor Windows NT para punto de venta, en las sucursales las PCS tienen diversas versiones de sistema operativo Windows (95, 98, etc.)

4.2 Servicios

En forma genérica podemos decir manejados por la red de comunicaciones de la que forma parte la red LAN que se analiza son de voz y datos.
La red LAN proporciona servicios de:

- Transferencia de archivos mediante FTP de la oficina central a las sucursales y de las sucursales a la oficina central, también se realizan transferencias de información mediante FTP de la oficina central a Internet y de Internet a la oficina central.
- Navegación WEB mediante http de las sucursales al corporativo para consulta de la intranet y para consulta de correos externos del personal de las sucursales, asimismo se usa la navegación WEB para consulta de paginas en Internet desde el oficina central.

- Conexiones TELNET desde la oficina central a las sucursales en ambos sentidos y de la oficina central a Internet y viceversa.
- Consulta de correo mediante los protocolos POP y SMTP de la oficina central al sitio del web hosting que hospeda el servidor de correo.
- Conexiones mediante sockets de TCP de las sucursales a la oficina central para realizar las autorizaciones de tarjetas de crédito.
- Se usan los servicios proporcionados por el conjunto de protocolos IP para el ruteo de paquetes a nivel Lan y entre la oficina central y sucursales.

4.3 Parámetros de operación

Las redes LAN tanto de la oficina central como de las sucursales tienen una topología física de estrella con tecnología de acceso al medio Ethernet, para la interconexión de los hosts se usan switches capa 2 y se tienen todavía como parte de los elementos de conectividad a nivel LAN.
En la oficina central se usa un direccionamiento de clase C con direcciones 192.0.0.0 y 192.0.100.0, este direccionamiento es usado por las dos subredes que sirven para interconectar en red a las computadoras, servidores y routers de las diferentes áreas de que se compone la empresa.
La red trabaja en un esquema plano por lo que no se realiza subnneting ni se tienen implementadas VLANs. El trafico generado por ambos segmentos de red 192.0.0.0 y 192.0.100.0 se mezcla en las dos subredes ya que estas dos direcciones son direccionadas a través del mismo router en el cual se encuentran configuradas por medio de subinterfaces lo que implica que el trafico de ambas subredes se mezcla en el mismo segmento físico.
La existencia de las subredes se debe a que con el direccionamiento inicial con una red clase C (192.0.0.X) se pueden tener hasta 254 hosts, con el crecimiento de usuarios llego el momento en que se agotaron el numero de hosts (254) disponibles la una red de clase C, como una solución rápida a este problema y para evitar problemas de cambio de direccionamiento se opto por implementar otra red también de clase C (192.0.100.X) para conectar en red a los nuevos usuarios y equipos. Para ello la segunda red se configuro como una subinterfaz en el router que funciona como gateway de la red primaria 192.0.0.X, por lo que el trafico de ambas subredes se conecta al mismo segmento físico.
Asimismo en la oficina central se tiene una tercera subred clase C 192.0.254.0 para el direccionamiento entre el servidor central Tandem y los servidores remotos de las sucursales de punto de venta, que se comunican para realizar la aprobación de pago con tarjetas de crédito.
El numero de hosts ya sea PCs y servidores en la oficina central son aproximadamente 300 hosts.
La red LAN de la oficina central alberga los distintos servidores a los que se conectan tanto los usuarios de la misma, como los usuarios y servidores de las sucursales.
Los usuarios y servidores de las sucursales se conectan a los servidores HP-9000, intranet, Antivirus, Recursos Humanos, correo también se accesa a Internet mediante IP a la oficina central y posteriormente se enrutan hacia el router de Internet (Cisco) las peticiones de navegación.
Los usuarios de la oficina central realizan conexiones mediante FTP y Telnet al sistema HP9000, realizan navegación mediante http al servidor de intranet. Las PCS se conectan al

servidor de antivirus para realizar la actualización del patrón de antivirus, se realiza la transferencia de correo a través del sistema HP-9000. Asimismo cada uno de los usuarios de la oficina central necesita comunicarse mediante Telnet o FTP a los servidores de punto de venta y HP9000 de cada sucursal.
Para el servicio de correo se tienen dos tipos de correo, el correo interno y el correo externo, el correo interno es usado únicamente para comunicación interna de la empresa, el correo externo es usado para el envío y recepción de mensajes a y desde Internet.
El correo interno es manejado por los servidores HP-9000 tanto de la oficina central como de las sucursales.
El correo externo es manejado por un servidor de correo espejo hospedado en la oficina central que a su vez realiza las peticiones y conexiones de envío y recepción de correos a Internet al servidor de correo hospedado con el proveedor de web hosting.
En las sucursales la red tiene una topología física de estrella con tecnología acceso al medio Ethernet, para la interconexión de los hosts se usan switches capa 2.
Para la conexión a Internet los usuarios deben autenticarse ante un firewall Netscreen para poder salir a Internet por medio del router Cisco que hace NAT para traducir las direcciones internas de la red local a las direcciones homologadas autorizadas por el proveedor, dicha conexión al proveedor es un enlace con PPP de 2 Mbps, el proveedor es UNINET.
La comunicación entre la oficina central y las sucursales se realiza mediante enlaces WAN Frame Relay con un CIR de 128 kbps y un BC de 192 kbps.
En las sucursales se tienen las redes con direccionamiento clase C 192.0.tienda.x y 195.1.tienda.x, que sirven para conectar en red a las computadoras, servidores y routers. La red 192.0.tienda.x es usada para la red local de PCs y la red 195.1.tienda.x es usada para la red local de punto de venta. Ambas redes son ruteadas a través de dos tarjetas de red en el router Motorola 6520 o 6560 de cada sucursal. En cada sucursal se tienen aproximadamente unos 70 usuarios, 50 serian PCs y servidores y los 20 restantes puntos de venta.
En las sucursales el sistema de punto de venta se comunica con la oficina central mediante IP para realizar las autorizaciones de pagos mediante tarjetas de crédito. Inicialmente cada sistema de la sucursal establece una conexión lógica de TCP (socket) con el equipo tandem en la oficina central y a partir de estas conexiones las peticiones de autorizaciones llegan al corporativo mediante IP. Los usuarios en cada sucursal se conectan a su servidor HP9000 para checar sus correos y comunicarse hacia otros servidores de la oficina central. A su vez en las sucursales debe existir conectividad por IP entre las dos redes existentes (punto de venta y centro de computo) para realizar transferencia de información entre los servidores de ambas redes.

4.4 Velocidades

En la oficina central las velocidades manejadas son de 10 Mbps y 100Mbps.
La estructura de elementos de conectividad ya sea en la oficina central o en las sucursales se compone de una mezcla de hubs, los cuales sabemos trabajan a 10 Mbps y switches con capacidad de trabajar hasta 100 Mbps.
En las sucursales también se manejan velocidades de 10 Mbps y 100 Mbps.

Se trabaja a 10 Mbps según se tengan conectadas PC's antiguas que no soportan trabajar a 100 Mbps o según esten conectados los hosts a puertos de hubs todavía existentes en el corporativo.
Se trabaja a 100 Mbps cuando se tienen PCS recientes y conectadas a puertos de los switches con capacidad autosense.
Las conexiones de las sucursales a la oficina central se realizan mediante enlaces Frame Relay que trabajan a una velocidad de 128 Kbps con un BC de 192 Kbps.
Para la conexión a Internet se tiene un enlace que trabaja a 2 Mbps.

4.5 Protocolos

En la parte física la red LAN usa el protocolo IEEE802.3 (Ethernet) para la comunicación a nivel físico y de enlace, en el nivel de red se usa el protocolo IP.
En la parte de aplicación se usan los protocolos POP3 y SMTP para mandar y recibir correo de la oficina central a las sucursales y de la oficina central a Internet.
Se usa el protocolo http para la navegación en el servidor de intranet y en Internet.
El protocolo FTP es usado para bajar y subir archivos de los servidores de la oficina central y de las sucursales.
Se usa el protocolo Telnet para realizar conexiones a los servidores y equipos de comunicaciones, desde la oficina central a las sucursales.
Asimismo se usa el protocolo ICMP para realizar pruebas de conectividad de servidores y hosts del corporativo y de las tiendas.
A nivel WAN se usan el protocolo Frame Relay para encapsular voz y datos entre la oficina central y sucursales, se usa el protocolo PPP para encapsular el trafico IP entre la oficina central y el proveedor de Internet.

4.6 Deficiencias actuales

El objetivo que se quiere alcanzar al usar la red LAN propuesta en este tema es usar dicha red como un modelo de referencia que nos ayude a determinar los cambios que tendrían que realizarse en una red en producción, con la intención de proponer un procedimiento general de los cambios necesarios que pudieran necesitarse en una red IPv4 para realizar la migración a IPv6.
Asimismo se busca probar el funcionamiento de IPv6 en un ambiente real, para poder decir con certidumbre si funciona o no, este nuevo protocolo.
Sin embargo podemos decir que actualmente esta red como se encuentra trabajando presenta problemas como:

- La red local de la oficina central presenta problemas de desempeño, ya que cuando se desea comunicar un hosts con otro por medio de IP, las maquinas reconocen la dirección de la maquina hosts con la que se quieren conectar por medio de broadcast que realiza el protocolo ARP para solicitar las direcciones MAC, debido a que en la red se tienen hubs como elementos de conectividad y no se implementa ningún mecanismo de subneting, este broadcast llega a todas las maquinas, incluso a routers y servidores inundando la red de trafico.
- La configuración de las direcciones IP en los equipos es del tipo estática por lo que a cada usuario se le asigna y configura su propia dirección IP. Debido a esta

configuración de las direcciones IP de los equipos de los usuarios en forma manual, los usuarios normalmente saben como y donde se configura la dirección IP y cuando salen de viaje, al regreso la gran mayoría se configura su dirección IP, sin tener los debidos cuidados de usar su IP asignada y respetar las de los demás, por lo que algunas veces duplican las direcciones con las de otro usuarios e incluso con las direcciones de servidores y/o equipos de comunicaciones provocando problemas como colisiones excesivas y por lo tanto caídas de la red.

- Lentitud cuando se realizan transferencias de archivos de una red a otra entre sucursales y la oficina central.
- Para el acceso a Internet se usa NAT para traducir las direcciones internas de la oficina central a las homologadas y cuando se desea establecer conexiones de video por ejemplo con Netmeeting, no se puede establecer conexión debido a la traducción de direcciones por lo que se tiene que configurar directamente una dirección IP homologada al host que desea establecer una conferencia de video por Internet con un punto remoto.
- No se tiene implementado algún sistema de seguridad entre las sucursales y oficina central, ni entre las redes de punto de venta y centro de computo.
- Hacia Internet la única seguridad que se tiene es la que proporciona el firewall para evitar accesos no autorizados, pero una vez que el usuario ha establecido una conexión desde la red local hacia Internet el acceso queda abierto sin ningún tipo de encriptación o autentificación de la información transferida desde o hacia Internet.

Requerimientos

La red que se propone para realizar una actualización requiere seguir usando los servicios que hasta ahora usa como son:

- Correo (protocolos smtp, pop)
- Internet (protocolo http)
- Trasferencias de archivos (protocolos ftp, tftp)
- Conexiones remotas (telnet)
- Videoconferencias con netmeeting, pcanywhere, real player, etc.

Se desea que el desempeño de la red no sea degradado por el uso de broadcasts, por lo que resulta muy interesante la idea de tener comunicación a nivel de enlace por medio de multicast exclusivos entre las maquinas en comunicación.

Se pretende que las asignaciones de direcciones de la maquinas sean dinámicas o autoconfiguradas por los equipos para poder evitar problemas como los que se generan cuando los usuarios realizan configuraciones manuales.

4.7 Topología con IPv6.

Esta propuesta de migración se ha tratado de realizar teniendo presente que la planeación, diseño e implementación de IPv6 debería realizarse en base a:

- Evitar la dependencia de actualización entre nodos, es decir que la actualización del nodo x se deba realizar antes que la del nodo y.
- Actualización paulatina para que la actualización de todos los nodos no se tenga que realizar al mismo tiempo. Para ello se debe poder actualizar una maquina a la vez e IPv6 debe poder estar disponible en diferentes productos en diferentes tiempos.
- Se debe permitir la transición de los sitios según su propia marcha o a su propio paso.
- Identificación de los requerimientos
    - Que tipos de aplicaciones se tienen (web, telnet, propias del cliente).
    - Alcance de la implementación (departamental, organización, Internet).
    - Tipos de sistemas.
    - Planeación de la transición.
    - Selección de mecanismos de transición.

La identificación de requerimientos determinara la selección de una estrategia de implementación. El administrador de red debería empezar seleccionando las aplicaciones y servicios que le gustaría ofrecer a través de IPv6. Debería identificar el router o routers en la red que necesitan ser de doble pila y que serán parte del dominio IPv6, usando los protocolos de ruteo IPv6 para comunicarse con las aplicaciones IPv6 y ya sea que se use IPv4 o IPv6 para comunicarse fuera del dominio. La elección del protocolo dependerá de si se esta conectando directamente a un ISP IPv6 o se usa una de las estrategias de implementación disponibles para transportar el trafico IPv6 sobre la infraestructura IPv4 existente a una red o dominio IPv6 remoto.

Planeación de la transición

La parte de planeación de la transición es importante para definir la estrategia de transición de IPv4 a IPv6 la cual lo recomendable es que inicie en los bordes de la red y se mueva hacia el núcleo de la misma. Esto permitirá controlar el costo de la implementación y las necesidades de las aplicaciones en lugar de realizar una actualización completa. Además en esta etapa el administrador de la red puede evaluar y probar IPv6 para checar el direccionamiento de extremo a extremo, la autoconfiguración, la QoS, la seguridad requerida por los nuevos ambientes de teléfonos móviles, o probar el espacio de direcciones expandido en sistemas telefónicos basados en IP, checar que el regreso a un direccionamiento global sea transparente a las aplicaciones. Para ello en esta etapa se pueden implementar dos puntos clave para evaluar y probar los productos y servicios IPv6:

- Configuración de un dominio IPv6 y conectarse a una red IPv6 remota como el 6Bone.
- Configurar dos o mas dominios IPv6 e interconectar estos sobre la infraestructura IPv4 existente.

También dentro de las actividades de evaluación al crear el dominio IPv6 se puede configurar un DNS que soporte ambos registros IPv4 e IPv6. Si hay necesidad de intercomunicar hosts IPv6-nativos con hosts IPv4-nativos se puede manejar un mecanismo de traducción de protocolo como NAT-PT en el router o un TCP-UDP Relay.

Como parte de la planeación de transición y antes de implementar IPv6 se puede empezar por registrarse para obtener una dirección IPv6 si se es un ISP o solicitar un prefijo IPv6 del ISP, configurar el DNS, seleccionar una política de administración de red y seleccionar los protocolos de ruteo.
El registro de la dirección IPv6 depende que la organización sea un ISP o una empresa, de si se esta registrado para estar en un ambiente de producción o se quiere ganar experiencia de IPv6 a través de la comunidad 6BONE y de la estrategia de implementación seleccionada.
El DNS debe ser configurado con un componente que soporte IPv6 y con una librería de resolución que maneje ambos tipos de registros IPv4 e IPv6.
Las primeras administraciones de red de routers de doble pila usan TFTP, ping, Telnet, traceroute con soporte completo de MIBs IPv6.
El soporte de protocolos de ruteo iniciales se enfocan sobre RIP, IS-IS y BGP, OSPFv3 y EIGRP para IPv6.
La siguiente secuencia de pasos se propone para realizar el proceso de actualización de IPv4 a IPv6 en la red propuesta.

- Selección del mecanismo de transición.
- Selección y acuerdo con un nodo pTLA o pNLA para realizar la conexión a la red IPv6 6BONE.
- Actualización del router(s) de Internet con la doble pila IPv4/IPv6.
- Configuración de túneles hacia el pTLA o pNLA para la comunicación hacia la red IPv6.
- Actualización de hosts con la doble pila IPv4/IPv6.
- Actualización de servidores con la doble pila IPv4/IPv6.
- Actualización de las aplicaciones a IPv6.
- Instalación de servidores adicionales como DNS y DHCP6.
- Actualización de ruteadores que conforman el backbone de la red interna.

En esta serie de pasos se tiene en cuenta que actualmente las pruebas que se puedan hacer de conexión hacia redes nativas de IPv6 se realizan a través de redes de pruebas ya que las de producción aun no son liberadas ni por institutos ni por ISPs, por lo que dichas conexiones tienen que ser a través de Internet con IPv4.
La secuencia ha sido propuesta tratando de que el nivel de afectación que pudiera provocar el proceso de migración al funcionamiento de la red y por tanto de la empresa se realice de lo externo o menos sensible a lo interno o más critico, la actualización de los equipos más externos debería afectar en menor medida a la empresa, puesto que internamente la red funciona normalmente sin que se entere que por ejemplo el router que da salida a Internet ha sido actualizado para trabajar con IPv6. Posteriormente internamente se puede continuar con la migración partiendo de los equipos más simples a los más sensibles o críticos para el funcionamiento de la red.
A continuación se trata de dar una justificación a la serie de pasos propuestos:

- Selección del mecanismo de transición.

La determinación del mecanismo de transición de IPv4 a IPv6 debería ser definida antes que cualquier actividad realizada para implementar IPv6, ya que como parte de la planeación de la estrategia de migración dicho mecanismo será usado durante todo el proceso.

Cuando los organismos encargados de definir los requisitos a ser cumplidos por las propuestas que se realizaran para implementar un nuevo protocolo de Internet de nueva generación pusieron como condición que las propuestas deberían incluir obligatoriamente mecanismos de transición.
Los mecanismos de transición son un conjunto de opciones de entre las cuales se puede elegir alguna o la combinación de algunas para hacer la transición a IPv6 con la menor interrupción posible ya que deben incluir alguna forma de coexistencia con la base IPv4 instalada.
Las estrategias clave para la implementación de IPv6 en el borde de una red involucran transportar trafico IPv6 sobre la red IPv4, permitiendo a los dominios IPv6 aislados comunicarse con cada uno de los otros antes de la transición completa a un backbone IPv6 nativo. Se puede usar tanto IPv4 como IPv6 a través de toda la red, desde los bordes hasta el núcleo, o se puede traducir entre IPv4 e IPv6 para permitir la comunicación de hosts manejando diferente protocolo. Todas las técnicas permiten que las redes sean actualizadas y la implementación de IPv6 gradual con poca interrupción de los servicios IPv4.
Para el proceso de migración se tienen diferentes opciones[1] para conectarse a Internet IPv6 como pueden ser:

- Uso direcciones compatibles de tipo ::w.x.y.z.
- Uso de la doble pila de protocolos IPv4/IPv6 en los nodos.
- Uso de túneles de IPv6 sobre IPv4 del tipo estáticos o configurados:

a) De ruteador a ruteador
b) De host a ruteador
c) De hosts a host
d) Túneles broker o de intermediario

- Uso de túneles dinámicos o automáticos 6to4 con prefijo 2002
- Uso de técnicas basadas en traductores IPv6 <-> IPv4:

a) NAT-PT
b) Otros traductores.

- Conexiones nativas de IPv6.

Debido a que durante tiempo indefinido muchos nodos necesitaran mantener una compatibilidad, todos los mecanismos que existen para realizar la transición a IPv6 están diseñados para ser usados por hosts IPv6 y routers IPv6 que tienen que seguir manteniendo una comunicación con hosts IPv4 y utilizar las infraestructuras de ruteo IPv4.
Estas opciones pueden ser usadas para realizar la conexión hacia Internet y también dentro de una red privada si se desean conectar subredes o sucursales IPv6 por medio de la estructura de IPv4.
Por ejemplo las direcciones compatibles podrían ser usadas para la conexión interna de la red privada, ya que para realizar la conexión hacia Internet esta opción esta ya descartada.
La opción de doble pila provee soporte completo para IPv4 e IPv6 en hosts y routers. La forma más directa de que los nodos IPv6 sean compatibles con nodos IPv4 nativos es manteniendo una implementación completa de IPv4 además de su implementación de IPv6 por lo que son llamados nodos IPv6/IPv4, al poseer la implementación de ambos protocolos tienen la capacidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4 y con los nodos IPv6 mediante los paquetes IPv6.

[1] Ver el tema 3.4.8 Mecanismos de transición a IPv6 y coexistencia con IPv4

Los sistemas con doble pila pueden ejecutar ambos protocolos IPv6 e IPv4, por lo que están conectados a ambas redes y necesitan direcciones IPv6 e IPv4, asimismo necesitan aplicaciones que hagan uso de ambos protocolos,
La técnica de los túneles encapsula los paquetes IPv6 con encabezados IPv4 que serán transportados a través de la infraestructura de ruteo IPv4, esta técnica permite comunicar nodos o redes IPv6 que se encuentran separados por infraestructuras IPv4 mediante la configuración de un túnel que forma un enlace virtual entre los extremos IPv6. Los paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de los paquetes IPv4. Los extremos de túnel serán creados con dos direcciones IPv4 y dos direcciones IPv6. Dichos túneles son transparentes a las aplicaciones y pueden ser configurados o automáticos.
Los túneles configurados son creados por configuración manual, como normalmente se realizan las conexiones hacia la red IPv6 del 6BONE.
Los túneles automáticos son creados dinámicamente por demanda y se establecen automáticamente mediante direcciones IPv6 IPv4-compatibles.
Sin embargo para realizar la conexión a Internet se pueden usar una combinación de nodos con doble pila de protocolo implementando un túnel para pasar el trafico por el enlace de Internet, cuyos túneles implementados pueden ser entre los routers de frontera de la red privada y el sitio TLA que nos permitirá tener acceso a Internet IPv6 o mediante túneles entre los hosts extremos que se quieren comunicar.
Esos túneles pueden establecerse con proveedores de túneles brokers (TLAs o pTLAs) que ofrecen este tipo de túneles específicamente para eso, con los cuales el establecimiento del túnel solo consta del intercambio de información de algunos datos necesarios y este se establece automáticamente.
O se pueden establecer los túneles dinámicamente por Internet donde el router de frontera de nuestra red generara el prefijo para el túnel dinámico con prefijo 2002 si tiene una dirección IPv4 publica homologada, dicha dirección será usada para convertirse en parte del prefijo y realizar el encapsulamiento de IPv6 en IPv4 para circular libremente por el Internet IPv4.
El uso de traductores permitirá la comunicación entre interlocutores IPv6 e IPv4, pero pueden presentar algunos problemas como la escalabilidad, esta técnica solo es recomendada si una aplicación no soporta ambos protocolos o se ejecuta en una maquina con una única pila o la red no soporta ambos protocolos, o en su defecto configurarla entre servidores para que la traducción sea transparente a los usuarios.
El uso de conexiones nativas de IPv6 debería ser el caso ideal si el servicio ya estuviera disponible comercialmente, podría usarse en caso de que toda nuestra red tuviera la capacidad de generar trafico IPv6 o en su defecto mediante el router de frontera de nuestra red que se encargue de convertir el trafico de IPv4 a IPv6 en caso de que la parte interna de nuestra red no sea en su totalidad IPv6.
Sin embargo el protocolo IPv6 puede ser usado en ambientes que no requieren mantener la interoperabilidad con IPv4, los nodos que se encuentren en esos ambientes no necesitan usar ni implementar los mecanismos de transición.

- Selección y acuerdo con un nodo pTLA o pNLA para realizar la conexión a la red IPv6 6BONE.

La determinación de la forma de conexión a Internet IPv6 consiste en seleccionar como vamos a conectarnos a la red IPv6. Esta parte no presentaría mayor problema si el servicio

de IPv6 estuviera disponible comercialmente, por lo que únicamente se tendrá que contactar al ISP que nos proporcione el servicio. En este caso como estamos en la primera fase de migración y como los enlaces nativos de IPv6 no se han liberado comercialmente, se tiene que buscar la forma de conexión a la red IPv6.
La selección del nodo TLA o pTLA dependerá de la existencia de ISP's que comercialicen enlaces nativos IPv6 TLAs o en su defecto para efectos de pruebas con el mundo IPv6 se deberá seleccionar la conexión por medio de túneles a nodos pTLAs.
Existen instituciones como la UNAM, el 6BONE o empresas que ofrecen túneles brokers con las cuales se pueden obtener prefijos delegados de los que les han sido asignados, después de realizar el tramite correspondiente con la entidad seleccionada y obtener un prefijo, se deberá configurar en conjunto con la entidad el túnel. Por este túnel pasara todo el trafico IPv6 y por medio de estas instituciones se redireccionara el trafico al backbone de IPv6.
Actualmente las empresas o instituciones que quieren probar IPv6 o conectarse al backbone de IPv6 realmente no buscan un ISP para obtener el servicio, se esta usando a entidades que ya han obtenido un bloque de prefijos y que a su vez fueron autorizadas para delegarlos a quien los requiera. Estas entidades ademas de que poseen prefijos para delegar, poseen una conexión directa al backbone de Internet IPv6 y es a través de ellos como se puede llegar hasta los nodos que componen la red actual de IPv6, es decir estas instituciones hacen la función de un router relay, el cual nos permite conectarnos a través de el hacia la red 6Bone y otros dominios IPv6 aislados.

- Actualización del router(s) de Internet con la doble pila IPv4/IPv6.

Es un hecho que durante el proceso de migración de IPv4 a IPv6 los equipos deberán ser actualizados para manejar ambas pilas de protocolos IPv4 e IPv6 para poder seguir comunicándose tanto con los dispositivos IPv4 y con los dispositivos IPv6. Esto en vista que la migración durara muchos años debido a la enorme infraestructura de IPv4 instalada.
Actualizar primeramente el equipo que permiten la conexión a Internet no afecta el funcionamiento interno de la red, es decir esta seguirá trabajando sin ser afectada por la actualización de un equipo que tiene mas interacción con el exterior de la red, en primer lugar por que la red interna solo usa el acceso a Internet en general para actividades que no son primordiales para la producción de la empresa, en segundo lugar las conexiones que realizan los hosts de la red interna hacia Internet continuaran realizándose en forma normal mediante la pila IPv4. Si los equipos que permiten el acceso a Internet manejan la doble pila y los hosts todavía sin actualizar hacen peticiones con IPv4 a Internet, los equipos de acceso a Internet preemitirán realizar la conexión como se hacia hasta antes de la actualización. Además la actualización inicial de estos equipos (firewalls, ruteadores, etc.) nos permitirá comprobar que la conectividad con IPv4 hacia Internet no se vea afectada, así como también nos permitirán probar desde este punto de frontera entre la red y el mundo externo que funcione la conectividad por medio de IPv6, Comprobar la conectividad a IPv6 desde este punto de nuestra red podría ser tomado como un indicador de que se puede proceder a continuar la migración de los elementos de la red interna, una vez probada la conectividad hacia la nueva red IPv6.

- Configuración de túneles hacia el pTLA o pNLA para la comunicación hacia la red IPv6.

La configuración de túneles será necesaria como una estrategia de migración y conectividad hacia IPv6, ya que se puede usar el enlace actual de Internet para configurar estos túneles como se haría normalmente con una VPN para interconectar dos sucursales a través del Internet, la ventaja de esto es que es transparente para nuestro proveedor de conexión a Internet. Es un hecho que todavía a estas fechas (2005) los grandes proveedores no están ofreciendo enlaces nativos de IPv6 por lo que el uso de túneles IPv6 a través del Internet IPv4 nos permitirá entre otras cosas:

- Evitar contratar o solicitar conexión por medio de IPv6 al ISP, lo que podría la generación de gastos elevados ya que además de que se nos proporcionaría tal vez un enlace adicional con IPv6 nativo, esto implicaría la migración de los ruteadores del backbone de la red del ISP a IPv6 cuyos gastos de migración tendrían que ser absorbidos por el usuario final, lo cual en estas primeras etapas de pruebas y conexión probablemente no resulte tan atractivo.
- Con el uso de los túneles aunque con un mayor overhead en los paquetes tendremos conectividad IPv6 sin costo alguno por el mismo enlace que se tiene contratado.

Esto será temporal hasta que los ISP tengan disponibles comercialmente los enlaces nativos de IPV6.

- Actualización de hosts con la doble pila IPv4/IPv6.

Una vez que la conectividad IPv6 externa ha sido implementada y se ha comprobado que funciona podemos empezar a realizar la actualización de los hosts en este punto estamos refiriéndonos a las maquinas de los usuarios comunes o PCs y probablemente servidores de aplicaciones comunes como servidores de correo, Intranet, antivirus que por el tipo de sistema operativo que utilizan la actualización es factible, no los servidores que son elementos críticos del sistema. La actualización de los hosts es realizable, ya que la gran mayoría de los proveedores de los sistemas operativos han ya implementado en su software la doble pila de protocolos. Para esto tenemos que checar si existe una versión del sistema operativo que incluya IPv6 o parche que realice la actualización, y antes de realizar la actualización del software tendríamos que verificar que las características del hardware de los hosts tengan la capacidad de soportar los requerimientos de recursos que requiera una nueva versión de sistema operativo, en caso de que no tengan capacidad de soportar los requerimientos como pueden ser las maquinas más antiguas, estas se pueden dejar trabajando con IPv4 hasta que termine su vida útil y sean completamente renovadas, el dejar estas maquinas con IPv4 no deberá afectar en nada la operación de la red ya que por eso estamos en la fase 1 de la migración que consiste en manejar una doble pila de protocolos por lo que los equipos actualizados podrán seguir comunicándose sin ningún problema con los equipos que no pueden realizar el cambio.

- Actualización de servidores con la doble pila IPv4/IPv6.

Los servidores por ser los elementos más críticos que componen una red deberán ser de los últimos en ser actualizados ya que estos equipos por ser más robustos y por el papel desempeñado de proporcionar servicios a todos los usuarios de la red, pueden verse mas afectados o afectar el funcionamiento de la red si requieren que para su actualización

tengan que realizarse toda una nueva recarga de software. Tal vez la sola aplicación de algún parche pudiera requerir un reinicio de estos para que se apliquen los cambios y se reconozca al nuevo protocolo. Por todo esto, estos equipos deberían ser de los últimos en ser actualizados, en este caso estamos hablando de servidores sensibles para la producción como servidores para tarjetas de crédito, cajas de punto de venta, etc. Servidores del tipo correo electrónico, intranets, de antivirus, etc., por el tipo de sistema operativo que manejan, ya funcionan con IPv6 y la actualización de estos equipos tal vez pudiera ser vista como si se realizara la constante actualización de un sistema operativo Windows para reparar bugs.

- Actualización de las aplicaciones a IPv6.

Las aplicaciones son una de las partes que más interesan a las empresas ya que estas representan la parte con la que el usuario final interactúa, puesto que un usuario no sabe si trabaja con IPv4, IPv6, direcciones de 32 bits de longitud o de 128 bits, etc., el usuario solamente ve la interfaz de las aplicaciones con la que desarrolla su trabajo.
Además si únicamente se actualiza la pila de protocolos de un servidor a nivel de red, de nada servirá si las aplicaciones no pueden manejar cualquiera de esas dos pilas ya que seguirán funcionando únicamente con IPv4.
Un gran numero de aplicaciones de uso comercial, como un navegador de Internet (Internet Explorer o Netscape), o una aplicación de correo como (Outlook), están siendo actualizadas para manejar IPv6, por lo que se tiene que consultar con el fabricante si se tienen versiones de ellas actualizadas para el manejo de IPv6.
Por otra parte si las aplicaciones son desarrolladas por la misma empresa habrá que trabajar con los desarrolladores para que modifiquen las estructuras o sockets de esas aplicaciones.

- Instalación de servidores adicionales como DNS y DHCP6.

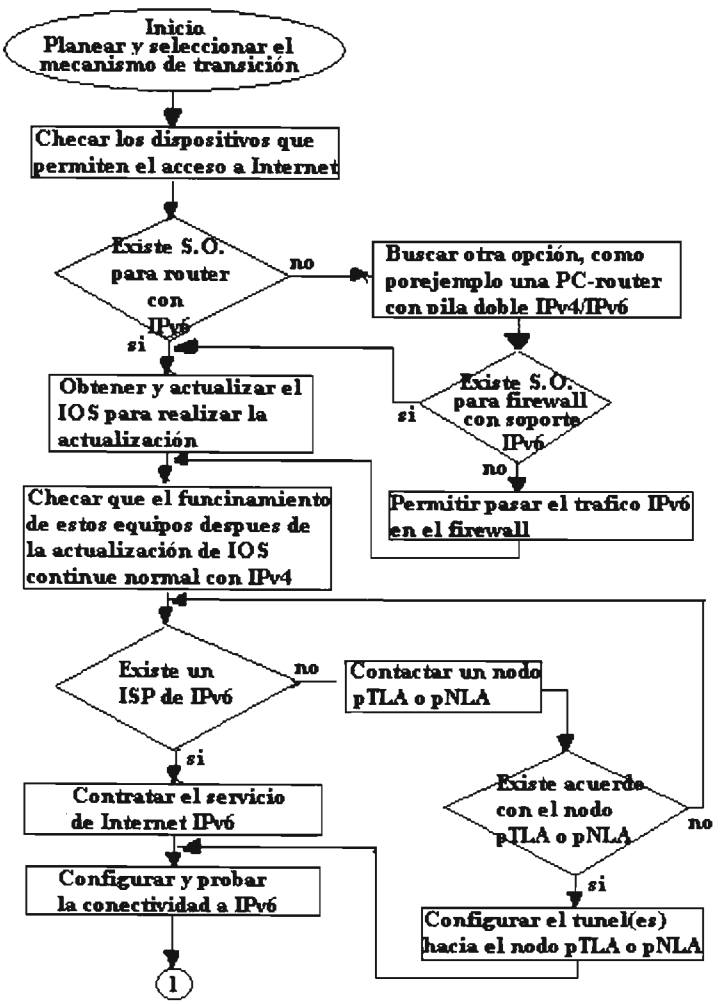
Tal vez se tendrán que instalar otros servidores que se requieran para poder hacer uso de IPv6, por ejemplo si internamente en la red no se maneja un servidor DNS y una vez actualizados los hosts de la red local se requieren comunicar entre ellos por medio de IPv6, lo más recomendable es el uso de nombres en lugar de direcciones IPv6 por el problema que implica manejar longitudes mas largas y en formato hexadecimal de las direcciones IPv6, lo que resultaría muy difícil o casi imposible, para lo cual ahora con IPv6 se hará necesario también para la comunicación interna la instalación de un servidor DNS, actualmente los servidores públicos instalados en Internet y comúnmente usados para IPv4 ya manejan registros AAAA y resuelven los nombres de sitios en direcciones IPv6. Por otro lado si se desea usar la autoconfiguración de direcciones IPv6 del tipo stateful, se requerirá manejar un servidor DHCPv6 para realizar esta tarea.

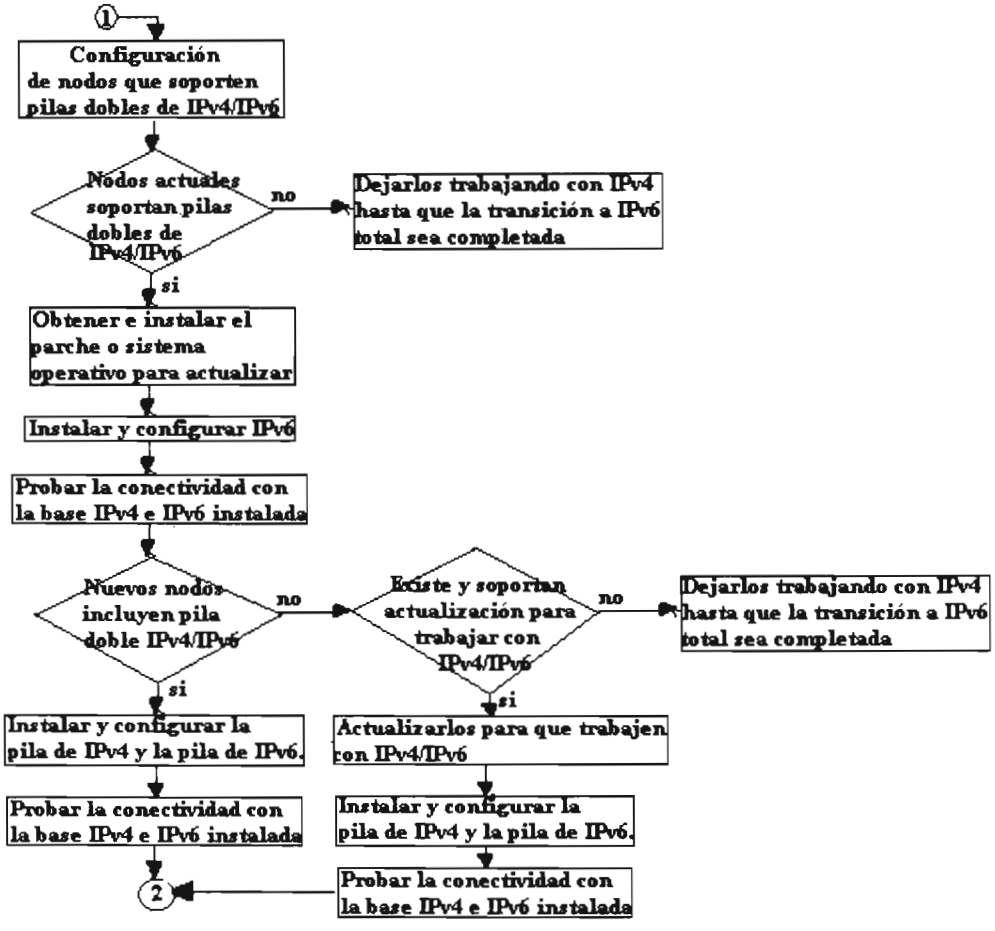
- Actualización de los ruteadores del backbone de la red local.

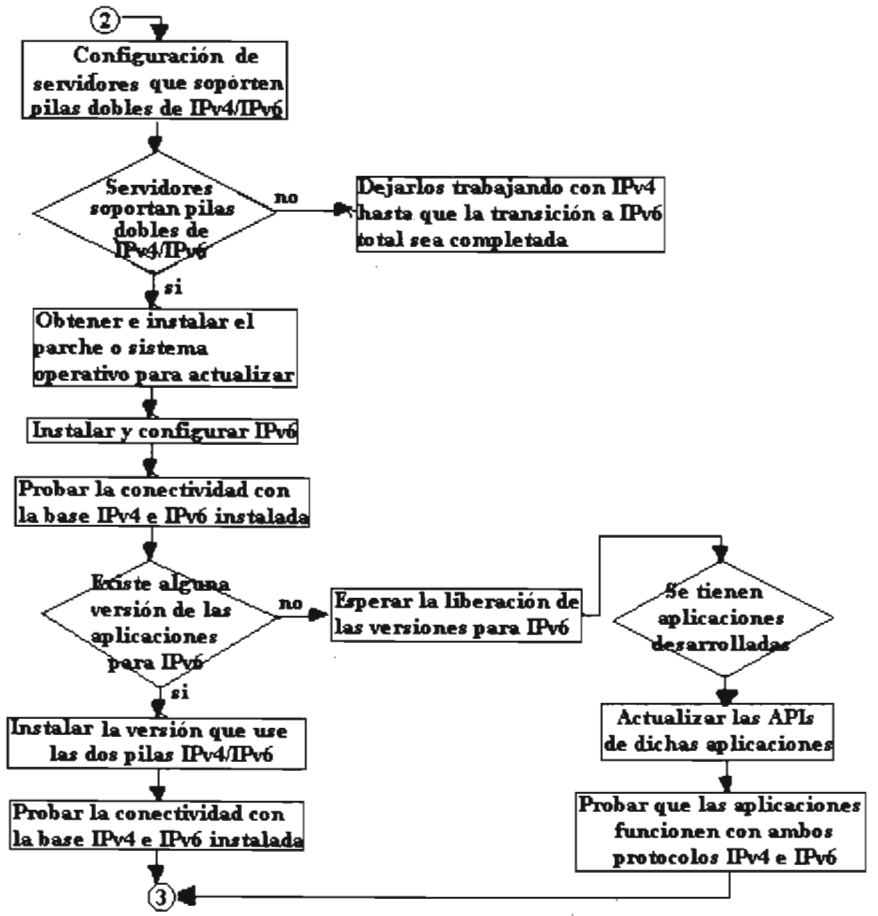
Los últimos equipos en migrar serian los ruteadores y equipos de interconectividad que componen la red interna, debido a la función más delicada que tienen de mantener los diferentes subredes que componen a la red comunicadas y por el costo que pudiera representar la actualización de estos.

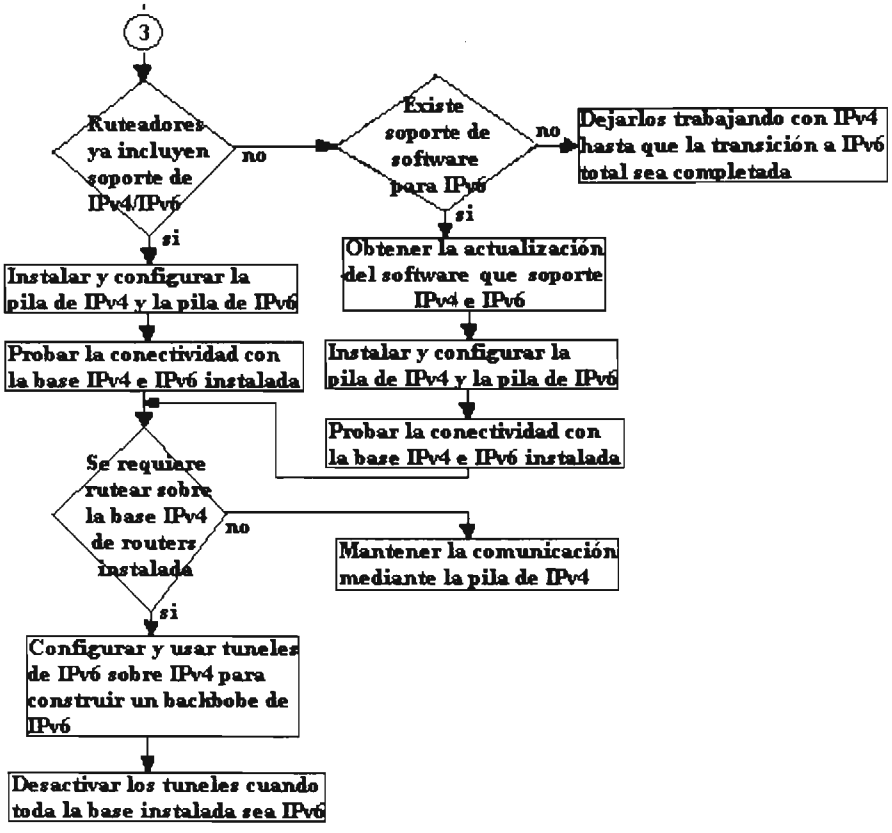
Diagrama de flujo para la transición inicial de IPv4 a IPv6

La secuencia que se propone para realizar la transición inicial de IPv4 a IPv6 se muestra en el siguiente diagrama de flujo:




1
Configuración de nodos que soporten pilas dobles de IPv4/IPv6
Nodos actuales soportan pilas dobles de IPv4/IPv6
no
Dejarlos trabajando con IPv4 hasta que la transición a IPv6 total sea completada
si
Obtener e instalar el parche o sistema operativo para actualizar
Instalar y configurar IPv6
Probar la conectividad con la base IPv4 e IPv6 instalada
Nuevos nodos incluyen pila doble IPv4/IPv6
no
Existe y soportan actualización para trabajar con IPv4/IPv6
no
Dejarlos trabajando con IPv4 hasta que la transición a IPv6 total sea completada
si
si
Instalar y configurar la pila de IPv4 y la pila de IPv6.
Actualizarlos para que trabajen con IPv4/IPv6
Probar la conectividad con la base IPv4 e IPv6 instalada
Instalar y configurar la pila de IPv4 y la pila de IPv6.
2
Probar la conectividad con la base IPv4 e IPv6 instalada


2
Configuración de servidores que soporten pilas dobles de IPv4/IPv6
Servidores soportan pilas dobles de IPv4/IPv6
no
Dejarlos trabajando con IPv4 hasta que la transición a IPv6 total sea completada
si
Obtener e instalar el parche o sistema operativo para actualizar
Instalar y configurar IPv6
Probar la conectividad con la base IPv4 e IPv6 instalada
Existe alguna versión de las aplicaciones para IPv6
no
Esperar la liberación de las versiones para IPv6
Se tienen aplicaciones desarrolladas
si
Instalar la versión que use las dos pilas IPv4/IPv6
Actualizar las APIs de dichas aplicaciones
Probar la conectividad con la base IPv4 e IPv6 instalada
Probar que las aplicaciones funcionen con ambos protocolos IPv4 e IPv6
3



El diagrama trata de llevar una secuencia aplicada a la migración en dos sentidos: por un lado tratando de realizar la migración de lo menos sensible al funcionamiento de la red a lo mas critico para la operación y funcionamiento de la misma y por otro lado que esa misma secuencia implique una menor mínima inversión a una mayor. Los primeros puntos que tratan de actualizaciones para las conexiones a la red de Internet IPv6 de hosts, servidores y aplicaciones la inversión puede ser mínima ya que en la mayor parte es solamente actualización o parches de software, si desde alguno de estos puntos se encontraran problemas de conectividad o funcionamiento con el protocolo IPv6, se podría detener la migración sin haber invertido demasiado, hasta llegar a los últimos pasos en los cuales se propone instalar nuevos servidores o un cambio total de equipos de ruteo.

4.8 Selección del mecanismo de transición

Como mecanismo de transición se decidió usar la combinación de la técnica de la doble pila y la técnica de los túneles.
El uso de la técnica de doble pila se decidió implementar tanto en hosts, servidores, aplicaciones y routers para mantener la idea de compatibilidad y funcionalidad con IPv4 en todo momento, ya que esta es una red en producción, es decir si cada elemento que se actualiza o migra soporta ambas pilas, dicho elemento podrá seguir conectado a la red IPv4

manteniendo la comunicación con los elementos aun no actualizados y podrá seguir con su función que realizaba.
El uso de túneles también se decidió utilizar en vista de que para tener comunicación hacia la red IPv6 por medio del Internet el uso de los túneles es la única opción si no se tienen disponibles comercialmente enlaces nativos de IPv6. Los túneles también podrían ser usados internamente dentro de la red si es que se tiene necesidad de comunicar subredes IPv6 a través de la Intranet formada por la red local.
Estas técnicas del manejo de los dos protocolos y el uso de túneles se probaron mediante un laboratorio de pruebas conectado a la red LAN propuesta, este laboratorio se formo con un conjunto de 5 maquinas funcionando como hosts, routers y DNS todos manejando la doble pila de IPv4/IPv6, aunque el laboratorio de pruebas implementado estaba conectado al mismo segmento físico de la red de producción, estos equipos formaban 3 subredes independientes a la red LAN de producción sobre la cual estamos trabajando, como muestra la Fig. 4.8.1

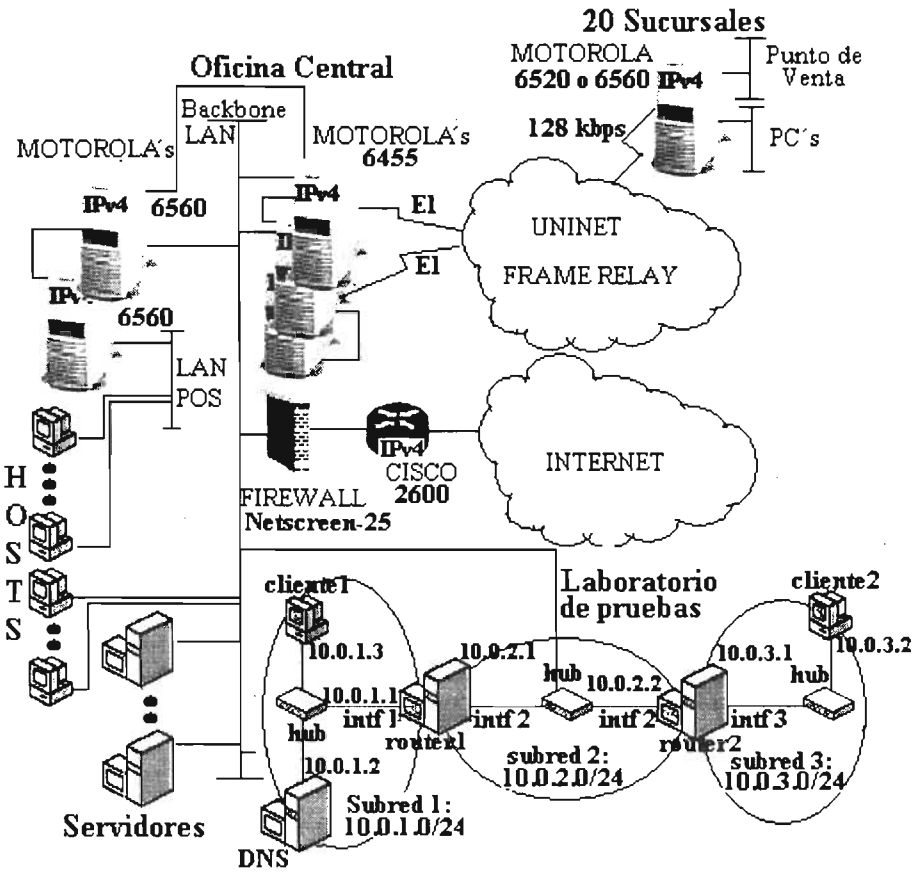


Fig. 4.8.1 Laboratorio de pruebas conectado a la red que se desea migrar

Este laboratorio es una propuesta de Microsoft para realizar pruebas, se uso este esquema por que todas las maquinas de la red tienen como sistema operativo Windows XP.
Se conecto dicho laboratorio a la red local para realizar pruebas[2] con diferentes esquemas y direcciones de este, que inicialmente nos permitieron familiarizarnos con el funcionamiento

[2] Véase el anexo A donde se tienen los diferentes esquemas de pruebas realizadas con el laboratorio

de IPv6 en un ambiente practico partiendo de las bases teóricas estudiadas, la mismas pruebas nos permitieron probar el cumplimiento y funcionamiento de algunos conceptos teóricos, también con el laboratorio implementado se hizo pasar trafico IPv6 encapsulado a través de equipos de la red sin actualizar y que no manejan IPv6 (como la base de ruteadores Motorola instalada, firewall, router de Internet) para probar por un lado que el transito de trafico IPv6 través de estos equipos se realice sin problema alguno y por otro lado que la compatibilidad entre equipos con IPv4 y equipos con IPv6 funcione, algunas implementaciones también nos permitieron hacer pruebas hacia sitios IPv6 a través del enlace de Internet normal, lo que nos permitió constatar que existe un gran numero de sitios IPv6, equipos con soporte IPv6 como los DNS públicos, routers relay, proveedores de túneles brokers, paginas que permiten la conexión ya sea con IPv4 o IPv6, etc. Se configuraron túneles dinámicos para probar el avance de la infraestructura actual en IPv6, es decir con una dirección IPv4 publica homologada se autoconfiguraron direcciones globales 2002 que son ruteables en Internet y para lo cual usamos una conexión lógica al ruteador relay de Microsoft como gateway para tener conexión al Internet IPv6 en vez de solicitar una conexión por túnel estático y una asignación de prefijo por parte de un nodo pTLA o pNLA la UNAM o los túneles brokers.

El stack de IPv6 de XP soporta la configuración de seguridad IPSEC con una administración simétrica de llaves con los protocolos AH y ESP en una forma básica ya sea en modo túnel o transporte con al algoritmo de autentificación HMAC-MD5, se configuraron manualmente las políticas de seguridad y las asociaciones de seguridad ya que XP aun no soporta la configuración dinámica de asociaciones de seguridad con IKE.

Con este laboratorio conectado al backbone de nuestra red se implementaron diferentes esquemas para probar la conectividad con IPv6, con el se probo la conectividad en la red localmente mediante direcciones autoconfiguradas link local, conectividad entre diferentes subredes IPv6 con direcciones site local, pruebas entre subredes diferentes a través de una Intranet IPv4 con direcciones isatap y v4-compatibles, se configuraron direcciones publicas y homologadas en las PCs routers y se conecto al Internet mediante el firewall y el cisco para tener direcciones unicast de agregación global 6to4 autoconfiguradas.

Los diferentes esquemas a su vez se probaron aplicando seguridad con IPsec usando los protocolos ESP y AH, además que se instalo y uso la resolución de nombres con IPv6 con la maquina que funcionaba como DNS.

Para realizar las pruebas se usaron aplicaciones como PING, Ping6 Tracert, Tracert6, Pathping, Telnet, FTP y http que son los protocolos mas utilizados en Internet.

Las maquinas trabajaban con Windows XP y Windows 2003 server. Se hicieron las pruebas básicamente con estos sistemas operativos ya que toda la infraestructura en la red en cuestión cuenta con maquinas de reciente adquisición las cuales todas tienen el sistema operativo Windows XP.

Se hicieron las pruebas hacia Internet mediante túneles 6to4 para lo cual se direcciono todo el trafico encapsulado en IPv4 al router relay 6to4 de Microsoft 6to4.ipv6.Microsoft.com que se encuentra disponible para tales efectos. Se instalo en cada maquina el software analizador de protocolos Ethereal para capturar el trafico IPv6.

La idea de implementar este laboratorio de pruebas fue como parte de la planeación de la implementación de IPv6.

4.9 Selección y acuerdo con un nodo pTLA o pNLA para realizar la conexión a la red IPv6 6BONE.

Antes de implementar IPv6 se puede empezar por registrarse para obtener una dirección IPv6 si se es un ISP o solicitar un prefijo IPv6 del ISP
El registro de la dirección IPv6 depende que la organización sea un ISP o una empresa, de si se esta registrado para estar en un ambiente de producción o se quiere ganar experiencia de IPv6 a través de la comunidad 6BONE y de la estrategia de implementación seleccionada.

Registro de un ISP
Los registros deben obtener una asignación de direcciones IPv6 unicast de agregación global que permite agregar las direcciones hacia arriba a través de las organizaciones e ISPs, estas se componen de un prefijo de ruteo global de 48 bits dentro del rango 2000::/3, un identificador de subred de 16 bits y un identificador de interfaz de 64 bits en formato EUI-64.
El registro como un proveedor de producción usa el proceso RIR. Los ISPs solicitan la asignación de un sub-TLA del registro regional pertinente APNIIC, ARIN o RIPE-NCC.

Registro de una empresa
Para usar IPv6 en un ambiente de producción, se solicitan direcciones IPv6 de ISPs apropiados. El ISP debe proporcionar un prefijo de ruteo de topología publica para la dirección unicast global IPv6, permitiendo crear una dirección apropiada al sitio como parte del proceso de configuración del router.
Como parte de la obtención de experiencia con IPv6, la opción es ser miembro de la comunidad 6Bone, es decir, convertirse en un sitio final de un ISP 6Bone. Se debe seleccionar un proveedor local ya que se debe configurar un túnel IPv4 desde el router IPv6 al punto de entrada de la red 6Bone. Se contacta al proveedor elegido usando la información en el registro 6Bone para un acuerdo de conexión. Una vez que se tiene un acuerdo de conexión se debe crear una entrada en el registro 6Bone que proporcione información para poder realizar la conexión, tener direcciones asignadas y ser contactado en caso de problemas. El ISP proporcionara el prefijo de ruteo externo como un ambiente de producción y el proceso de configuración del router determina el resto de la dirección.

En este punto lo ideal seria la contratación del servicio nativo de IPv6 con algún proveedor, pero todo parece indicar que los proveedores de servicios de Internet aun no tienen este servicio disponible comercialmente.
Actualmente se ha formado una red mundial de pruebas de IPv6 conocida como 6BONE a la cual están conectadas instituciones educativas y fabricantes. Para podernos conectar al 6BONE se requiere que alguien nos transporte nuestro trafico hacia la red, para lo cual necesitamos encontrar algún nodo del 6BONE dispuesto a hacerlo. Los nodos del 6BONE que pueden dar conexión a otros y delegar prefijos se llaman pTLA o pNLA según el nivel que ocupen en la jerarquía de ruteo.
La conexión directa al 6BONE o delegación de prefijos para usuarios finales en IPv6 ya no esta permitida, esta delegación de prefijos solamente es proporcionada a grandes ISPs e instituciones educativas, los cuales a su vez podrán estar capacitados o autorizados para

delegar porciones de sus prefijos a los usuarios que lo requieran. Por ejemplo el LACNIC que se encarga de administrar las direcciones IPv4 e IPv6 para América Latina y el Caribe indica las siguientes características a cumplir para realizar la asignación inicial de IPv6:

a) Ser un ISP.
b) No ser un sitio o usuario final.
c) Documentar un plan detallado sobre los servicios y la conectividad en IPv6 que se ofrecerá a otras organizaciones.
d) Anunciar en el sistema de rutas inter-dominio de Internet un único bloque que agregue toda la asignación de direcciones IPv6 recibida, en un plazo no mayor de 12 meses.
e) Ofrecer servicios de IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 meses.

LACNIC administra el bloque 2001:1200::/23 y las organizaciones que cumplan con los requisitos anteriores recibirán un mínimo de asignación de /32. Esta asignación de bloque IPv6 por parte de LACNIC no tiene costo durante los dos primeros años.

De los nodos pTLA o pNLA existentes actualmente, muchos pueden ser contactados directamente por Internet para solicitar la conexión y realizar los tramites necesarios.

En México existen como ejemplos de pTLA´s instituciones como el tecnológico de Monterrey ITESM, la Universidad de Guadalajara UdeG y la UNAM. Asimismo como sTLA´s tenemos al ITESM y la UNAM. Así como los ISP´s Avantel, Axtel, Protel, UNINET, aunque estos últimos son proveedores no se tiene aun conocimiento de que proporcionen ya el servicio comercial.

Entre las instituciones la UNAM es de las que más ha proporcionado acceso al backbobe de IPv6 y puede delegar prefijos de pruebas, estos como puede verse en su pagina www.ipv6.unam.mx son proporcionados a empresas e instituciones que los soliciten para pruebas, los prefijos para producción aun no los libera.

La figura 4.9.1 nos muestra la red IPv6 de pruebas de la UNAM y algunas redes de pruebas conectadas a la misma:

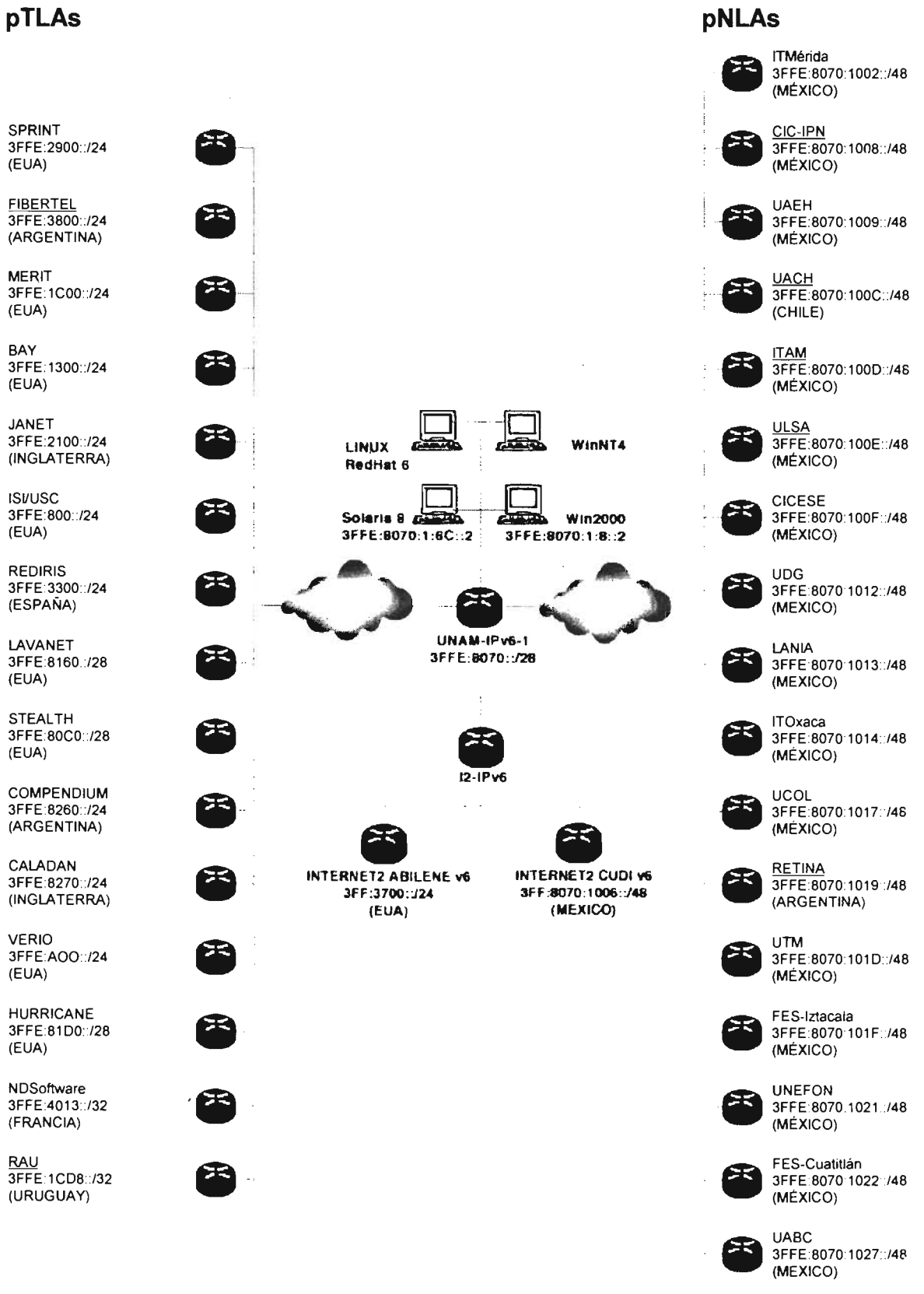


Fig. 4.9.1 Redes de pruebas conectadas a la UNAM.

Esta es la red IPv6 de pruebas obtenida directamente de la pagina IPv6 de la UNAM en la cual se especifica que:

- Esta disponible para pruebas nacionales e internacionales.
- Se pueden configurar túneles y delegar espacios de direcciones IPv6

También tenemos en la Fig. 4.9.2 la red IPv6 de producción de la UNAM:

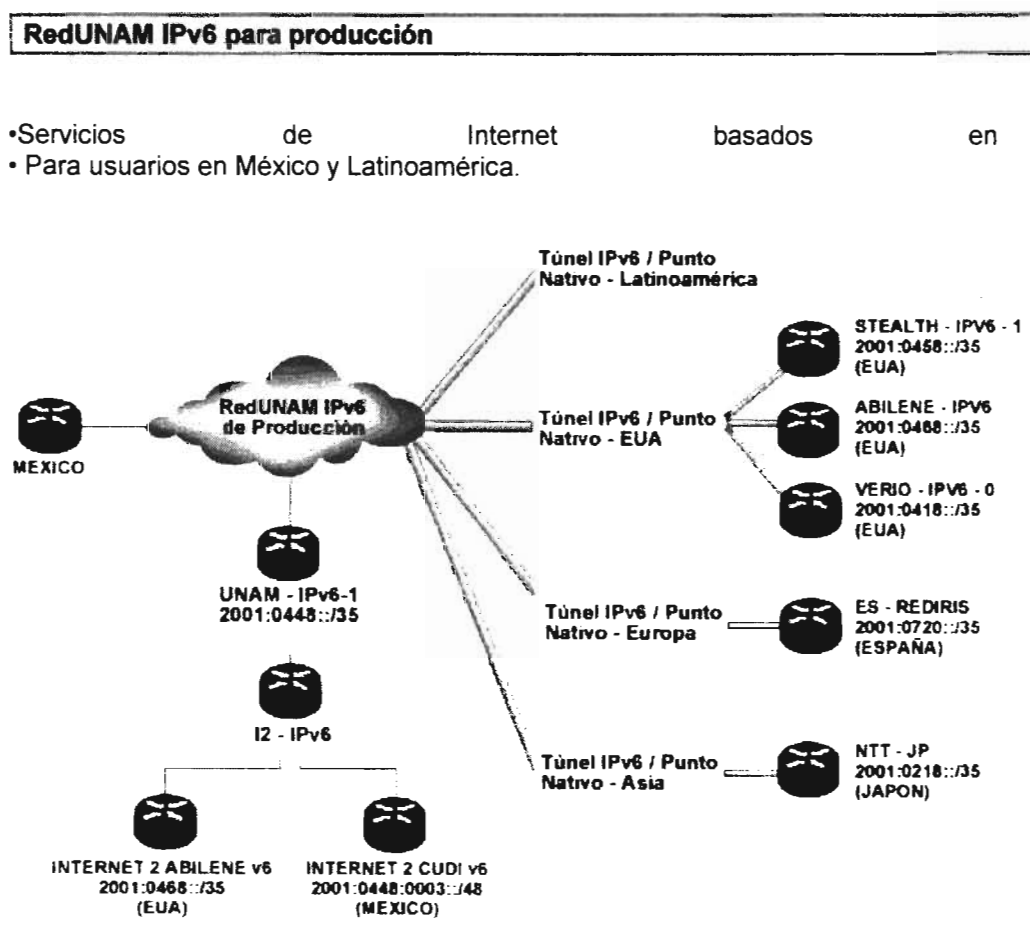


Fig. 4.9.2 Topología de la red IPv6 de producción de la UNAM

Podemos ver la topología de la red y el prefijo que le fue asignado a la UNAM y que proporciona servicios de IPv6 para México y América Latina, aunque en la misma pagina de la UNAM se indica que delegación de prefijos de este tipo no esta disponible por el momento.

Una vez que se ha seleccionado el nodo pTLA o pNLA se debe proceder a contactar al personal que administra el nodo, esto se puede realizar normalmente en la pagina de Internet del nodo seleccionado, para lo cual se deberá llenar un formato en el que se hace la solicitud de conexión y delegación de prefijos

Para poder realizar la conexión a IPv6 por medio de la UNAM se debe llenar el procedimiento de solicitud de direcciones IPv6, el cual es mostrado en la Fig. 4.9.3:

SOLICITUD DE BLOQUE DE DIRECCIONES IPV6.
SOLICITUD DE CONEXIÓN MEDIANTE TUNEL.

| TUNELES DELPid SOBRELPid | PAGINA DIRECCIONES |

INFORMACIÓN DE LA INSTITUCIÓN O EMPRESA:

Nombre Completo:

Dependencia:

Siglas:

Dirección Postal

Calle y No.:

Colonia:

Del. o Municipio:

Ciudad: ---

Estado: --- r por favor):

País: Otro (especificar por favor):

Código Postal:

CONTACTO ADMINISTRA

NIC-Handle:

Título:

Nombre (s):

Apellido Paterno:

Apellido Materno:

Puesto:

E-mail:

Teléfono:

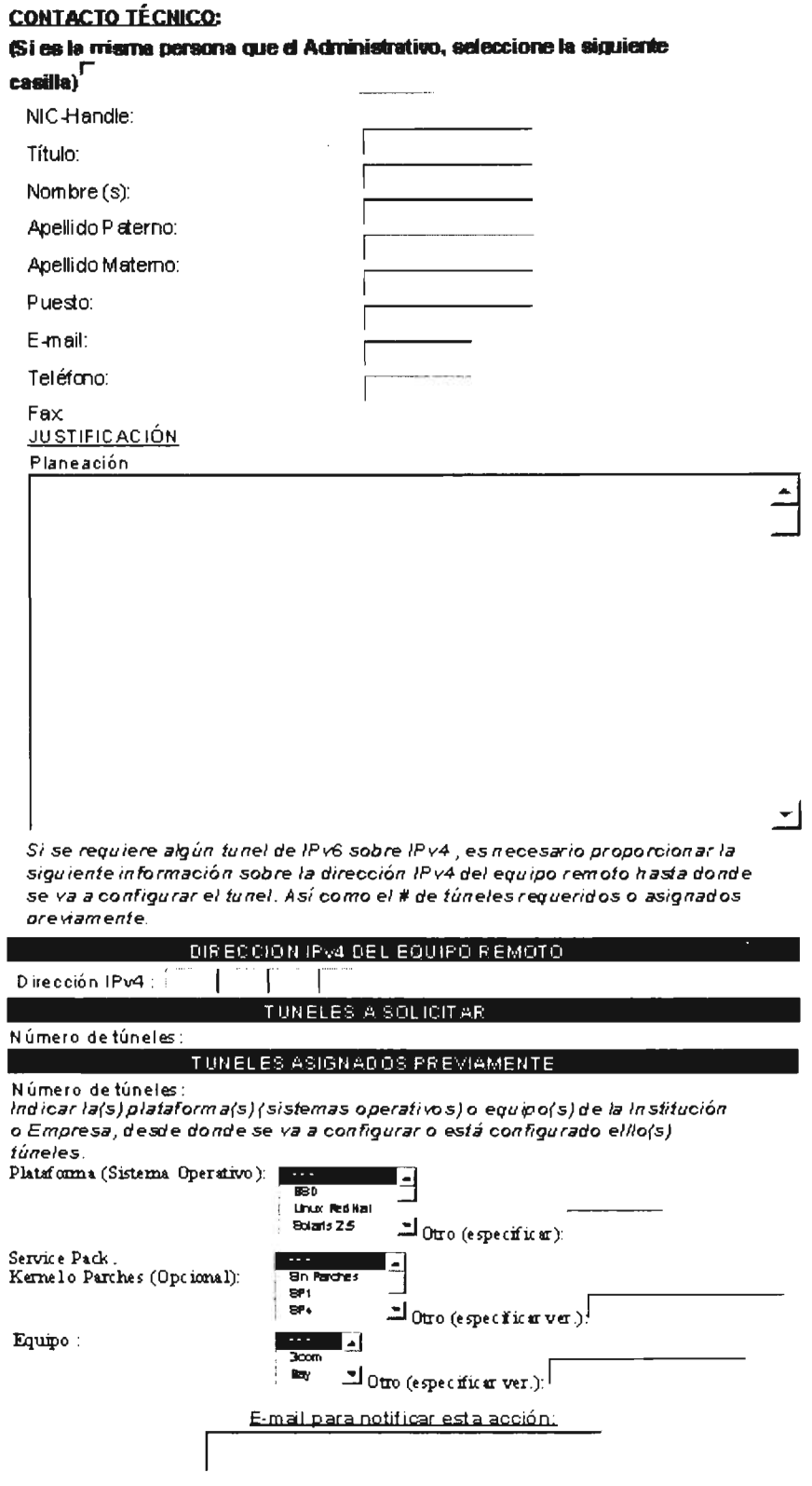


Fig. 4.9.3 Formato para solicitud de un bloque de direcciones IPv6 y conexión mediante un túnel a la UNAM.

En general para cualquier nodo pTLA o pNLA los datos que se deben indicar de nuestra parte al administrador del nodo son:

- La dirección IPv4 publica de nuestro router.
- El numero de sistema autónomo (AS) si es que disponemos de uno.

4.10 Actualización del router de Internet con la doble pila IPv4/IPv6.

El mecanismo de transición de uso de la doble pila de protocolos IPv4/IPv6 se propone teniendo en cuenta que IPv4 seguirá existiendo y deberá poder interactuar con IPv6, para lo cual la migración propuesta se basa en el manejo de ambos stacks de protocolos IPv4 e IPv6 así como el uso de técnicas basadas en túneles para comunicar redes IPv6 a través de redes IPv4.

El primer paso de la migración será la actualización de los equipos que nos permiten tener conexión a Internet. Para accesar a Internet tenemos un equipo firewall Netscreen y un ruteador de la marca Cisco.

Las pruebas realizadas con el laboratorio de pruebas conectado a la red nos permitieron darnos cuenta primeramente que el firewall no dejaba pasar el trafico IPv6 aunque estuviera encapsulado con IPv4, esto puede ser debido a que el firewall al ser su función la inspección profunda de paquetes y observar el numero de protocolo 41 en el campo protocolo del encabezado IPv4 automáticamente desecha este tipo de paquetes, por lo que determinamos que esa es una de las primeras actualizaciones que se debe hacer. En este caso se debe ver con el fabricante Netscreen si se tiene alguna versión de sistema operativo para manejar IPv6 o mover la configuración del equipo para que deje pasar este tipo de trafico, o en su defecto cambiar el equipo.

La primera opción queda descartada ya que aunque el fabricante ya da soporte completo a IPv6 en muchos de sus equipos, el modelo de firewall que se tiene en la red que es un Netscreen NS-25 con versión de software 4.0.3r1.0 es uno de los modelos del fabricante que aun no soportan IPv6. El fabricante ya ha liberado la versión de software ScreenOS 5.0 que soporta ambos protocolos IPv4/IP6, túneles, traducción de protocolos, etc., pero solamente para modelos más grandes, por lo que habría que esperar que en un futuro cercano libere la actualización para este modelo.

La segunda opción de entrada es la más rápida y a nuestro alcance, es decir se tendrán que activar políticas en el firewall para dejar pasar los paquetes con protocolo 41.

Sin embargo también tenemos la opción de proponer el cambio del modelo Netscreen-25 a un modelo que maneje IPv6, entre los modelos que manejan IPv6 se encuentran el 5XT y el 204, el 5XT es un modelo con menor capacidad que el que se tiene actualmente, que aunque cuenta con las mismas interfaces físicas, internamente su capacidad es menor que el 25.

Por su parte el modelo Netscreen-204 es dos modelos arriba del 25 con capacidad 4 veces mayor al que se tiene, por lo que este seria la opción más viable en caso del cambio del modelo.

Por su parte el ruteador cisco tiene la versión de software 12.1(2)T, esta versión solo maneja IPv4 por lo que tendría que actualizarse a una versión de las que Cisco ha liberado para manejar tanto IPv4 como IPv6.

Cisco es una de las empresas que más ha trabajado en el desarrollo de IPv6 y ha liberado ya versiones del sistema operativo o IOS con la característica de IPv6 a partir de la 12.2, actualmente la que ya sido liberada para ambientes de producción es la 12.3. El nuevo despliegue tecnológico IPv6 de Cisco son el Cisco IOS 12.3T y 12.2S.
Cisco ha ofrecido soporte para IPv6 desde mayo del 2001 cuando libero el IOS 12.2T, este era un sistema operativo para que los clientes experimentaran con IPv6. Actualmente IPv6 esta disponible en muchas versiones de Cisco IOS, por lo que las recomendaciones para el soporte de IPv6 son:
Producción General: Cisco IOS 12.3M.
Core ISP y NREN: Cisco IOS 12.0S para los routers Cisco de las series 12000 y 10720.
Infraestructura empresarial e ISP: Cisco IOS 12.2S
Acceso de banda ancha: Cisco IOS 12.2B.
Concretamente el router Cisco podríamos actualizarlo con la versión de IOS 12.2(2)S o superior.
Por lo tanto en este paso la actualización que se tendría que realizar se muestra en la Fig. 4.10.1:

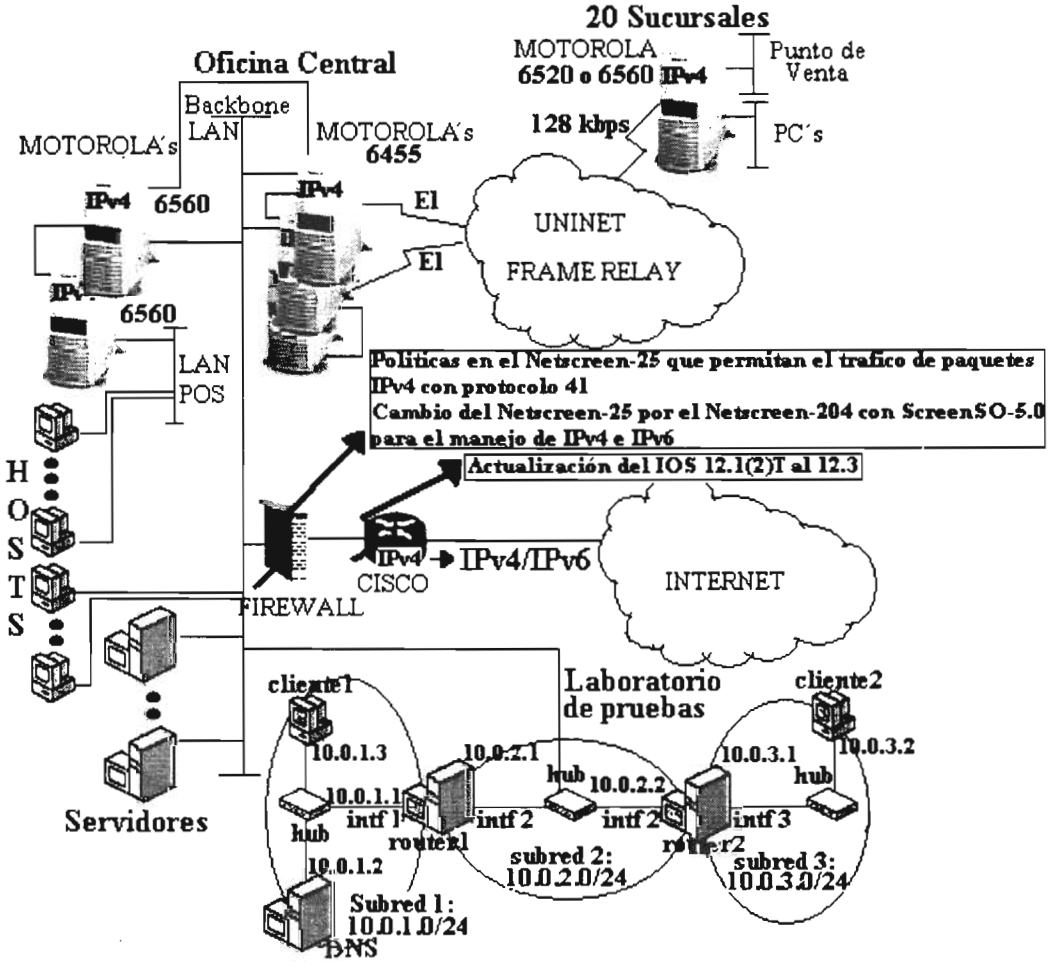


Fig. 4.10.1 Actualización de la conexión a Internet para manejo de IPv6

La configuración de las políticas en el firewall se puede realizar sin ningún problema y la actualización del sistema operativo o IOS del ruteador Cisco si se tiene algún contrato de

mantenimiento con Cisco podemos hacer la descarga de la nueva versión del software de la pagina de cisco.
Como podemos ver se esta actualizando el router de acceso a Internet independientemente del resto de la red y sin afectar el funcionamiento normal, ya que con el equipo actualizado puede seguir trabajando normalmente, puesto que por medio de la pila IPv4 permitirá el trafico hacia y desde Internet y con la pila de IPv6 podrán realizarse la comunicación por medio de túneles a IPv6.
Para no mover la actualización del router cisco y tener que cambiar el firewall, también podríamos usar como opción un router en paralelo al router cisco de cualquier marca (cisco. Nortel, 3com, etc.) o incluso una PC router con algún sistema operativo que soporte IPv6 (BSD, Linux, Windows, etc.), con esta opción tenemos la conexión a Internet intacta y la conexión a IPv6 disponible también. De hecho esta seria una buena opción en caso de que existieran enlaces de IPv6 comerciales, donde lo más probable es que se nos proporcione un enlace adicional al que se usa para Internet, dicho enlace adicional tendría que ser recibido con otro equipo como se propone. Esta opción se muestra la Fig. 4.10.2

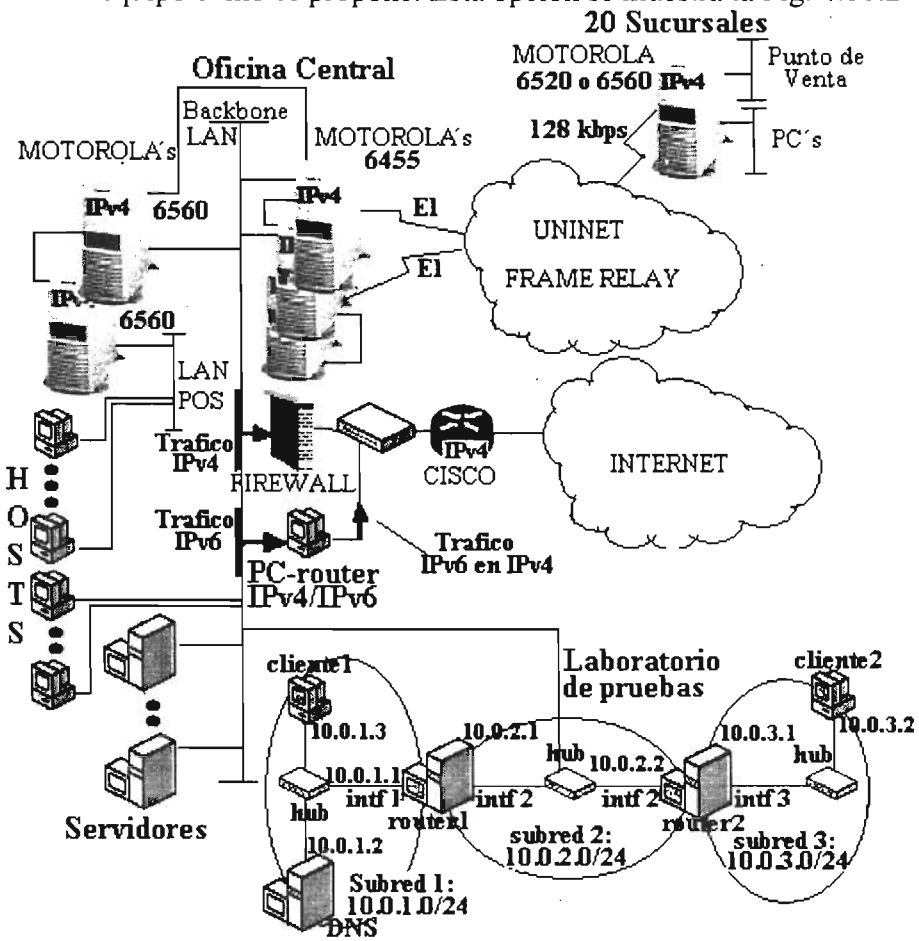


Fig. 4.9.2 Conexión opcional hacia Internet IPv6

En este caso como podemos ver ya sea que se decida poner otro router que seria la opción mas cara o una PC como router con dos tarjetas de red se configuraría con una dirección IPv4 publica homologada con lo cual ya tendría conexión hacia Internet.

Este equipo sería el que recibiría el trafico IPv6, lo encapsularía y lo mandaría a través de la infraestructura IPv4.
La ventaja de sistemas como linux o BSD es que estos sistemas presentan ciertas facilidades o software para hacerlos funcionar como routers, con lo que se pueden realizar configuraciones propias de ruteadores como la configuración de protocolos de ruteo, sistemas autónomos, tuneles, etc., en equipos como Windows XP seria más fácil habilitar el ruteo mediante rutas estáticas para efectos de poder direccionar el trafico que llegue a este equipo desde la red local hacia Internet.
Dentro de las pruebas realizadas con el laboratorio, se dividió este laboratorio en dos subredes, una conectada por medio de una PC router con una dirección IPv4 publica conectada al enlace de Internet de 2 Mbps y la otra con la PC router conectada a Internet por medio de un enlace de prodigy de 512 kbps, con estos dos ambientes se hicieron pruebas desde las PCs que integraban cada una de las subredes para checar la conectividad hacia IPv6 y las pruebas no presentaban problema alguno, las dos PCs router que conectaban a las subredes a Internet encapsulaban el trafico con encabezados IPv4.
Esta conexión en paralelo al router cisco es opcional, pero para efectos de la migración de la opción de actualizar el IOS del router Cisco resulta mas útil para el funcionamiento real y futuro de la red.

4.11 Configuración de túneles hacia el pTLA o pNLA para la comunicación hacia la red IPv6

Una vez llenado y enviado por medio de la pagina de Internet el formato de solicitud de conexión y delegación de prefijos, se indica que se recibirá una respuesta para conocer el prefijo delegado así como los datos necesarios para configurar y levantar el túnel en el cual serán encapsulados los paquetes de IPv6 para poder pasar por el enlace de Internet hasta la red de la UNAM la cual nos reenrutara directamente al backbone de IPv6. Es decir la UNAM funciona como un router relay.
Los datos básicos que necesitaremos de nuestro nodo pTLA o pNLA son los siguientes:

- Dirección IPv4 de su router.
- Numero de sistema autónomo.
- Direcciones IPv6 para el túnel.
- Bloque IPv6 que nos será asignado.

La forma de conectarse a la red de IPv6 por medio del nodo de la UNAM es configurando un túnel entre nuestro equipo de ruteo que nos permite el acceso a Internet y el equipo de la UNAM, para ello bastara con tener un enlace a Internet y por lo menos una dirección IPv4 publica fija, el procedimiento para configurar el túnel y los datos son proporcionados por los administradores o personal de contacto de la institución, pero básicamente para crear el túnel se deben asignar las direcciones IPv4 local y remota y luego configurar la interfaz del túnel como punto a punto.
Con los datos necesarios se puede proceder a configurar en nuestro equipo de ruteo los parámetros necesarios para levantar un túnel con los datos que nos sean proporcionados.
En un router la serie de comandos para configurar el túnel es la siguiente:
1.- Una vez logeado como usuario privilegiado entrar al modo de configuración, es decir se teclea el comando: (configure terminal).

2.- Entrar a la configuración de la interfaz túnel:
(interface tunnel <numero de túnel>).
3.- Configurar la dirección IPv6 que tendrá nuestro lado del túnel con el comando:
(ipv6 address prefijo-ipv6/longitud-prefijo [EUI64])
4.- Se configura la dirección IPv4 de nuestro lado del túnel:
(tunnel source {dirección IP | numero de tipo}
5.- Se configura la dirección IPv4 del otro extremo del túnel:
(tunnel destination dirección-IP)
6.- Se configura el modo del túnel IPv6 sobre IPv4:
(tunnel mode ipv6ip).
7. Se termina la configuración de la interfaz túnel.

El bloque de direcciones IPv6 que se asigne para nuestra red normalmente tiene un prefijo de 48 bits (/48) de longitud por lo que tendremos 48 bits para identificar a nuestra red y 16 bits disponibles para configurar nuestras subredes, con lo cual podemos tener una cantidad enorme de dispositivos conectados a cada red. Así es como podemos conectarnos a la red IPv6 a través de la UNAM en México.
Se puede hacer directamente con 6BONE que es la red de pruebas de IPv6, solamente que esta estipulado que las direcciones IPv6 solamente serán asignadas a grandes ISPs los cuales se encargaran de delegar los prefijos a los clientes que lo requieran, para las instituciones que requieren un bloque de prefijos delegados por el 6BONE directamente las condiciones que deben cumplir son variadas y difíciles de cumplir para un usuario final u organización pequeña.
Esta conexión también puede realizarse contactando a alguna otra empresa o institución que este autorizada a delegar prefijos como rediris, o empresas que manejan túneles brokers como freenet6. En cualquier empresa o institución que se contacte para realizar esta conexión a IPv6 hasta el momento en todas se tiene que configurar un túnel de IPv6 sobre IPv4 por el cual pasara todo nuestro trafico IPv6, después de que nos proporcionan el prefijo nos indican los datos necesarios para realizar la configuración del túnel. Algunas empresas como freenet6 realiza la configuración del túnel automáticamente.
Además de configurar el túnel se debe habilitar el ruteo en nuestro router lo cual se puede hacer de dos formas:

- Manualmente mediante rutas estáticas.
- Automáticamente mediante protocolos de ruteo.

Lo más recomendable es usar ruteo automático mediante protocolos de ruteo básicamente por que los routers tienen la facilidad de implementar los protocolos, se ahorra trabajo y por que se deben probar los protocolos de ruteo con IPv6.
El ruteo estático se podría usar en el caso de que hayamos decidido implementar conectarnos a IPv6 con algún host que no tiene muchas facilidades para manejar protocolos de ruteo.
De esta forma con la pila de IPv6 disponible en nuestro equipo de acceso a Internet se puede proceder a levantar uno o más túneles con la organización o instituto con el que se haya establecido el contacto y realizar las pruebas pertinentes de funcionamiento de dicho túnel. Así el esquema de red se modifica en la forma mostrada en la Fig. 4.11.1:

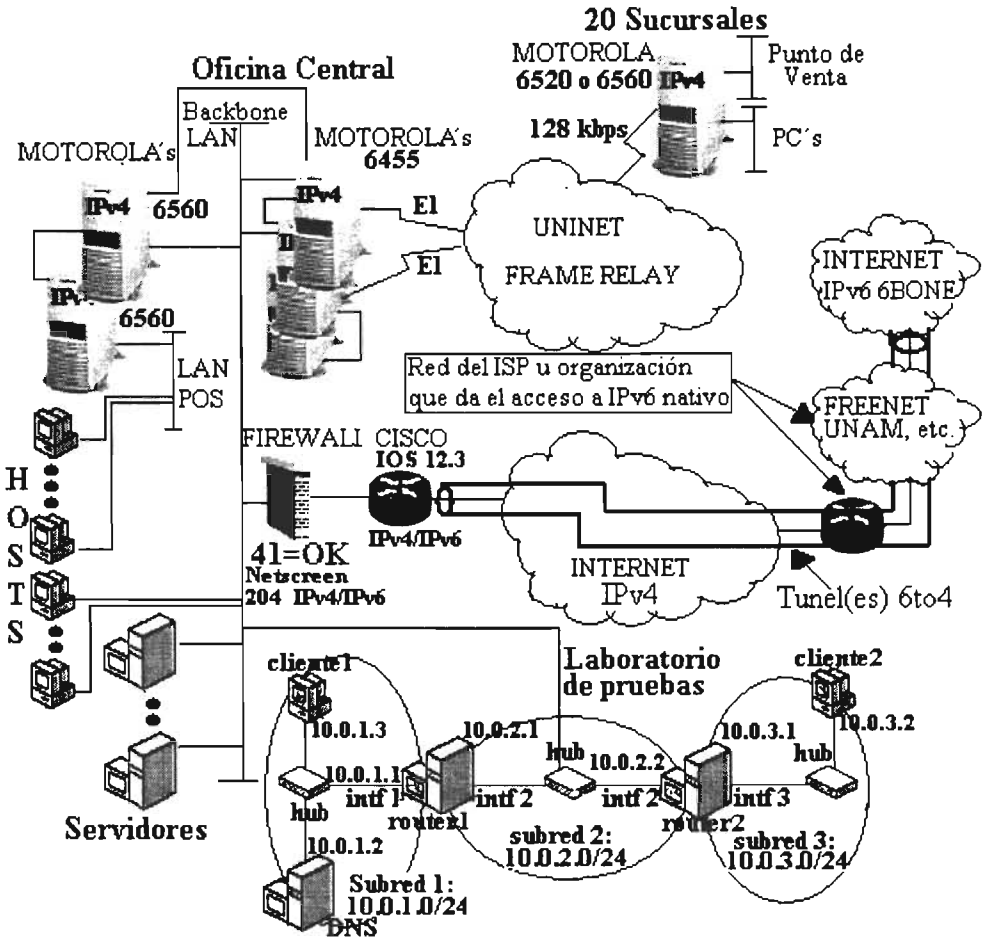


Fig. 4.11.1 Configuración de túnel(es) 6to4 hacia el nodo pTLA o pNLA.

Asimismo entre las varias técnicas de conexión actual a IPv6 se tiene la opción de usar túneles dinámicos los cuales se autoconfiguran automáticamente.
Los pasos en forma resumida para configurar un túnel automático en un router Cisco son:
1.- Una vez logeado como usuario privilegiado entrar al modo de configuración, es decir se teclea el comando: (configure terminal).
2.- Entrar a la configuración de la interfaz túnel:
(interface tunnel <numero de túnel>).
3.- Se configura nuestra dirección IPv4 que será la fuente del túnel automático:
(tunnel source {dirección IP | numero de tipo}
4.- Se configura el modo del túnel IPv6 sobre IPv4 automático:
(tunnel mode ipv6ip auto-tunnel).
5. Se termina la configuración de la interfaz túnel.

En nuestro laboratorio, entre las diversas pruebas realizadas se usaron túneles automáticos o dinámicos, para ello se usaron las PCs con dos tarjetas de red como ruteadores y se conectaron directamente a Internet configurando en su tarjeta que hace la conexión a Internet direcciones IPv4 publicas homologadas. Con Windows XP cuando se habilita la compartición de internet ICS (Internet Connection Sharing) en los equipos que funcionan

como routers automáticamente configuran un prefijo 6to4 global de la forma 2002:wx:yz (los octetos wx:yz son las direcciones publicas homologadas configuradas en las tarjetas de los equipos) y anuncian estos prefijos al resto de la red local provocando que los hosts se autoconfiguren con el prefijo anunciado y su identificador de interfaz del tipo EUI-64, las pruebas realizadas con túneles 6to4 automáticos se realizaron con el esquema de la Fig. 4.11.2:

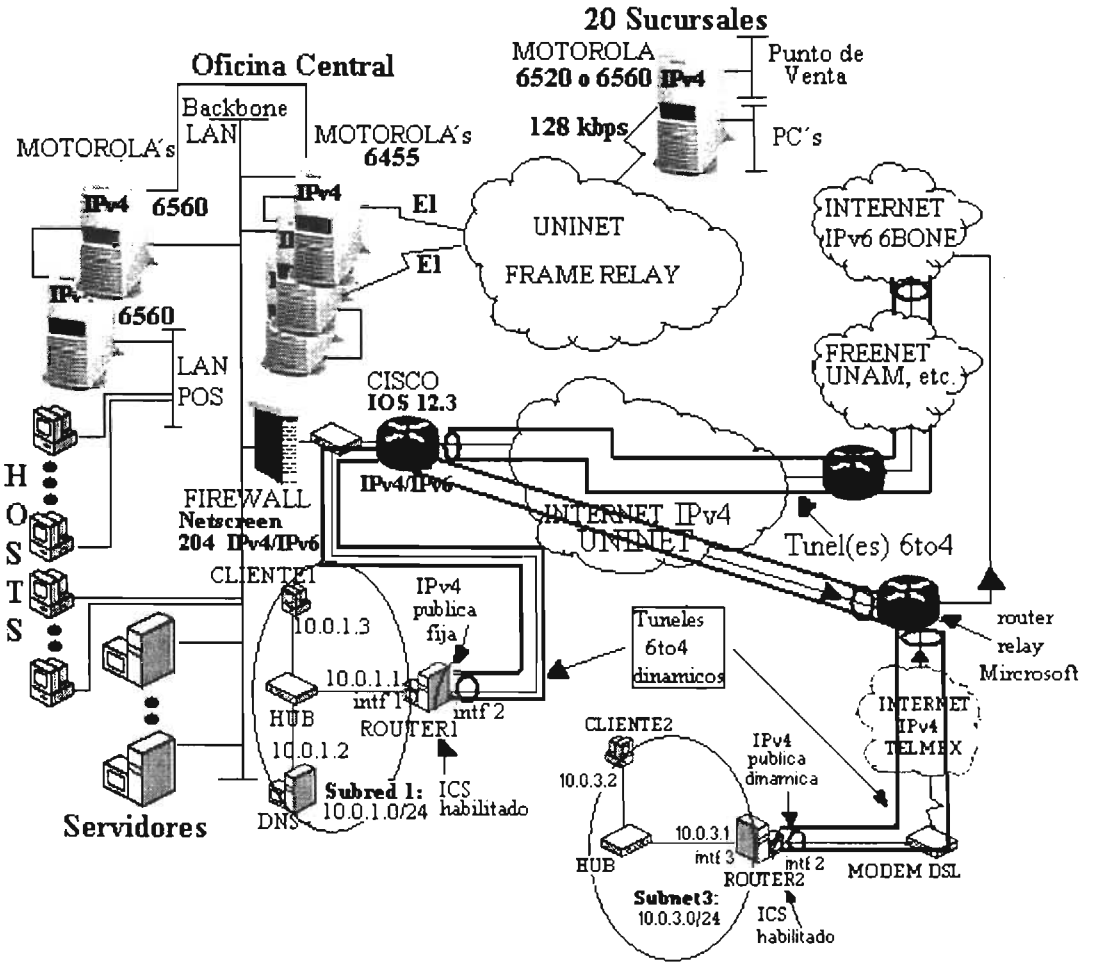


Fig. 4.11.2 Túneles automáticos 6to4 al router relay de Microsoft

En el esquema de la Fig. 4.11.2, podemos ver que se dividió el laboratorio para usar dos enlaces diferentes para estas pruebas, se conecto la subred 1 del laboratorio a Internet con el enlace usado por toda la red local que consiste de un enlace de 2 Mbps dedicado contratado con Uninet con lo cual se obtiene un grupo de 10 direcciones publicas homologadas para uso de la red, una de esas direcciones fue la que se configuro al router1, por su parte la subred 3 se conecto a Internet por medio de un enlace prodigy infinitum de 512 kbps contratado con Telmex con dirección IPv4 publica dinámica, con tener una dirección publica sea fija o dinámica e ICS habilitado los equipos que funcionaban como routers con el sistema operativo Windows XP automáticamente se configuran un prefijo 2002:wx:yz para lo cual usan sus direcciones publicas en la construcción del prefijo, el cual anuncian a los hosts de su subred local y los hosts toman el prefijo para autoconfigurarse direcciones globales 6to4.

También en los routers conectados a Internet router 1 y router 2 automáticamente se autoconfigura una ruta estática que dirige todo el trafico IPv6 (::/0) hacia el router relay de Microsoft (6to4.ipv6.microsoft.com) con el cual se realiza el proceso de tunelización, así todo el trafico que llega a nuestros routers 1 y 2 dirigido a sitios IPv6 se encapsula en un túnel con sus direcciones IPv4 publicas y se dirige al router relay de Microsoft que se encarga de hacer llegar ese trafico al destino mediante sus conexiones a la red IPv6.
Se hicieron las pruebas correspondientes hacia sitios IPv6 con ping, tracert, pathping, telnet, ftp y http y las pruebas fueron exitosas y el trafico fue capturado con el software ethereal.

4.12 Actualización de hosts con la doble pila IPv4/IPv6

Siguiendo con el principio de que la actualización sea independiente de un nodo a otro podemos proceder a actualizar los hosts que son la mayoría de los equipos de la red.
En este punto se realizaría la actualización del sistema operativo de las maquinas para que puedan manejar las dos pilas de protocolos IPv4 e IPv6, esto significa que para las maquinas cuya versión de sistema operativo exista actualmente la versión para IPv6 se realice dicha actualización, si dichas maquinas soportan la nueva versión sin tener que cambiar de hardware (actualizar el hardware de la maquina), en caso de que no exista una versión de sistema operativo para IPv6 o que por las características de la maquina se tenga que crecer para soportar una nueva versión de sistema operativo, la propuesta es dejar estas maquinas sin actualizar para que no generen una inversión hasta que sea necesaria.
En este caso en la red que estamos analizando todas las PCs que se encuentran conectadas a la red local son nuevas, y tienen como sistema operativo Windows XP, este sistema operativo ya soporta además de IPv4 la pila IPv6 como parte del sistema operativo, es decir no necesita ningún parche ni actualización, lo único que se tiene que realizar es instalar el protocolo de IPv6, este sistema operativo ya trabaja perfectamente con IPv6, lo cual lo pudimos constatar con las pruebas realizadas con el laboratorio conectado a nuestra red local, formado con PCS de la red en cuestión y que estaban en producción.
Si hubiéramos tenido el caso de no contar con esta ventaja de maquinas nuevas, y nuestras maquinas hubieran tenido algún sistema operativo anterior a XP, se tendría que realizar la actualización o parche de esos sistemas operativos.
Si se tuviera el sistema operativo Windows 95, 98 o anterior, las maquinas con este sistema operativo tendrían que ser actualizadas a otro sistema operativo ya que Microsoft no tiene pensado liberar un parche para instalar la pila de IPv6 en estas versiones. Aunque Trumpet ha implementado una versión Winsock de IPv6 para Windows 95/98/NT.
En el caso de que las maquinas que debieran ser actualizadas fueran de características de hardware que soportan la instalación de nuevas versiones de sistema operativo, ya que conforme se desarrollan nuevas versiones se requieren mas recursos, se podría proceder a la actualización, las maquinas que no pudieran ser actualizadas podrían seguir trabajando como están, recordemos que los equipos que si se están actualizando se comunicaran con IPv4 e IPv6, es decir ni los equipos con IPv4 quedaran incomunicados, ni los que manejen IPv6 formaran su subred aislada de comunicación, ya que estamos en la primera fase de migración que es la instalación de pilas dobles, cuyo objetivo es precisamente alentar y fomentar la actualización hacia IPv6 sin perder la comunicación con IPv4.

Por su parte si se tiene versiones como Windows NT, 2000 o posteriores se han liberado parches para que estas versiones ya manejen IPv6.
Las versiones de Windows XP y 2003 sever ya traen por default la pila IPv6 junto con la pila de IPv4.
Una vez actualizados los hosts a IPv6, la instalación de la pila IPv6 es muy sencilla, ya que se puede instalar desde el mismo entorno de red como se instalaría un nuevo protocolo.
Con la parte de IPv6 activada, no olvidando que la parte de IPv4 sigue funcionando normalmente ya que estamos en la una primera fase de migración propuesta que es tener la doble pila IPv4/IPv6, los hosts conectados a la red local ya pueden comunicarse inmediatamente entre ellos por medio de direcciones IPv6 del tipo link local.
En nuestro laboratorio de pruebas, montado con maquinas que tenían el sistema operativo Windows XP y 2003 Server de activar la pila de IPv6 inmediatamente se autoconfiguraron las direcciones de link local con el prefijo FE80::/10 y el identificador de interfaz EUI-64, las pruebas realizadas con direcciones de link local funcionaban perfectamente, aparte de que se seguían comunicando los hosts por medio de IPv4 como hasta antes de la activación de IPv6, con lo cual se continua cumpliendo el objetivo de realizar las actualizaciones independientemente y sin afectar el funcionamiento de otros equipos o de la red entera.
Nuestro esquema de red se puede modificar para indicar este punto como muestra la Fig. 4.12.1:

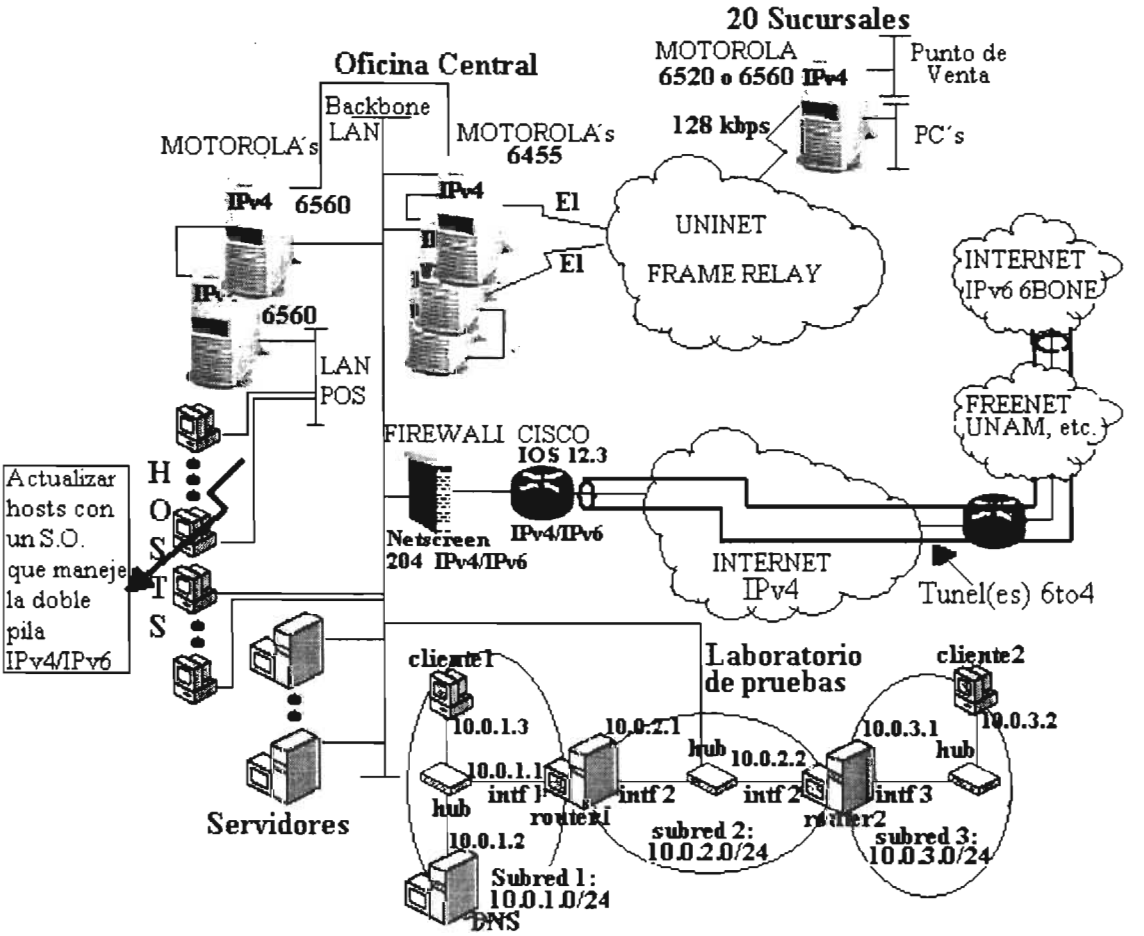


Fig.4.12.1 Actualización de los hosts con la pila doble IPv4/IPv6

Una vez que los hosts soportan ambas protocolos IPv4 e IPv6 y con el equipo que nos conecta a Internet anunciando su prefijo a la red local, los hosts pueden por autonfiguración crear su dirección IPv6 independientemente del direccionamiento IPv4 que se tenga en la red local, con lo cual el funcionamiento tanto local a la red como hacia Internet con IPv4 seguirá funcionando igual, mientras que el funcionamiento con IPv6 local y hacia el 6BONE también funcionara por su lado usando los túneles.

4.13 Actualización de servidores con la doble pila IPv4/IPv6.

Los servidores son de los equipos más críticos desde mi punto de vista ya que estos equipos son el corazón de una red desde los cuales y hacia los cuales fluye prácticamente todo el trafico generado en una red.
La red consta desde servidores de aplicaciones comunes como el de Intranet, antivirus, smtp y pop para correo, servidor de software, etc. Pero también tenemos otros servidores más críticos que son el HP 9000 y el servidor tandem para tarjetas de crédito.
Los primeros servidores mencionados (Intranet, antivirus, smtp y pop, de software) funcionan básicamente algunos sobre linux y otros ya sea con windows 2000 server o NT. Actualmente tanto en linux como en Windows los parches para trabajar con IPv6 están liberados y probados, por lo cual la aplicación de los parches a este tipo de servidores puede realizarse sin ningún problema y sin afectar su funcionamiento, la instalación de un parche en este tipo de equipos es muy común y en este caso el instalarles un parche para IPv6 puede verse como el proceso cotidiano de aplicar parches implementar mejoras o corregir fallas de software.
Respecto a los servidores más críticos tenemos dos opciones: primero verificar con el fabricante si tiene actualizaciones para el servidor en cuestión para la implementación de IPv6, así como el procedimiento para realizar esta actualización, por lo que se tiene que checar durante dicho procedimiento que no se interrumpa la actividad y funcionamiento de estos servidores o en segundo lugar dejar estos servidores trabajando únicamente con IPv4 hasta llegar a una etapa de madurez de trabajo con IPv6 ya que volvemos a recordar que los equipos que no se migren tal vez por mucho tiempo continúen comunicándose con los equipos actualizados gracias a las pilas dobles de IP. Así en nuestra red ese es el siguiente cambio. Fig. 4.13.1:

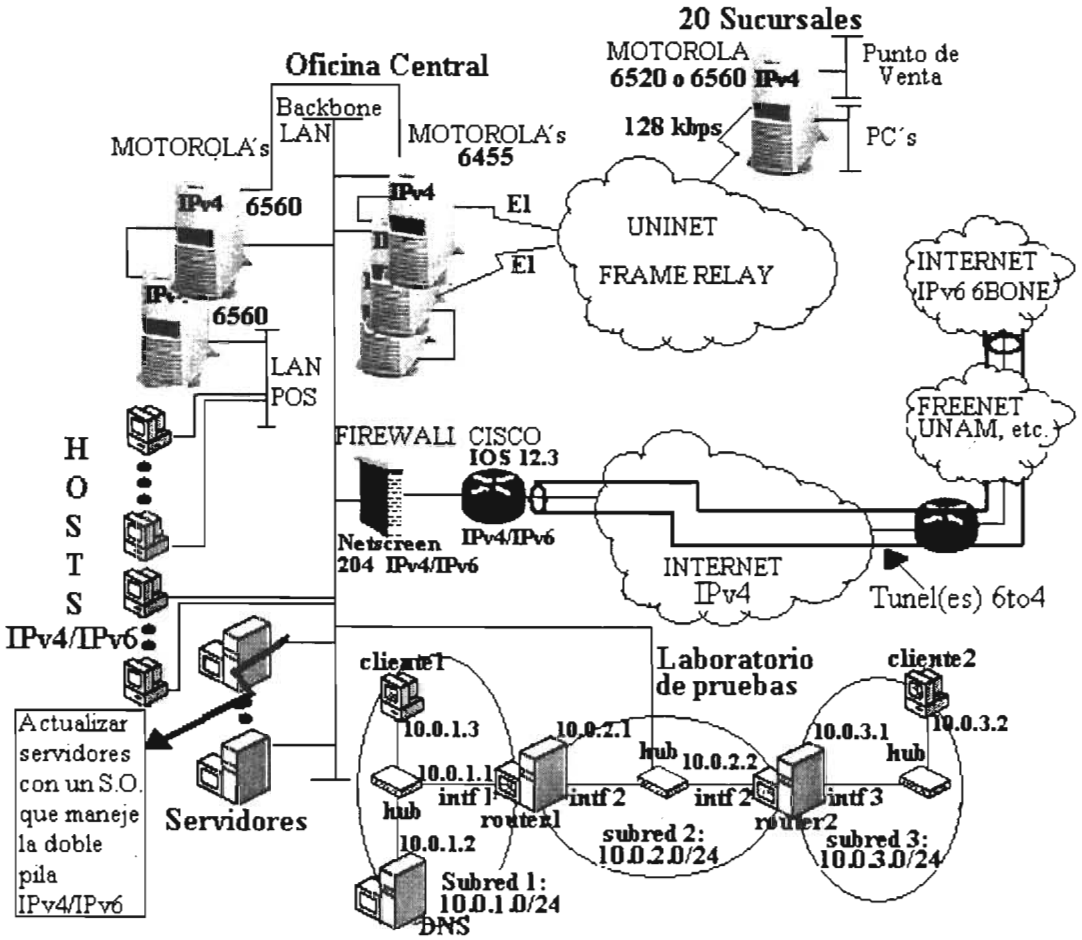


Fig. 4.13.1 Actualización de servidores con los protocolos IPv4 e IPv6

4.14 Actualización de las aplicaciones a IPv6

Una vez que la actualización de las pilas de protocolos de los hosts y servidores han sido actualizadas tenemos que realizar la actualización de las aplicaciones, Fig. 4.14.1.

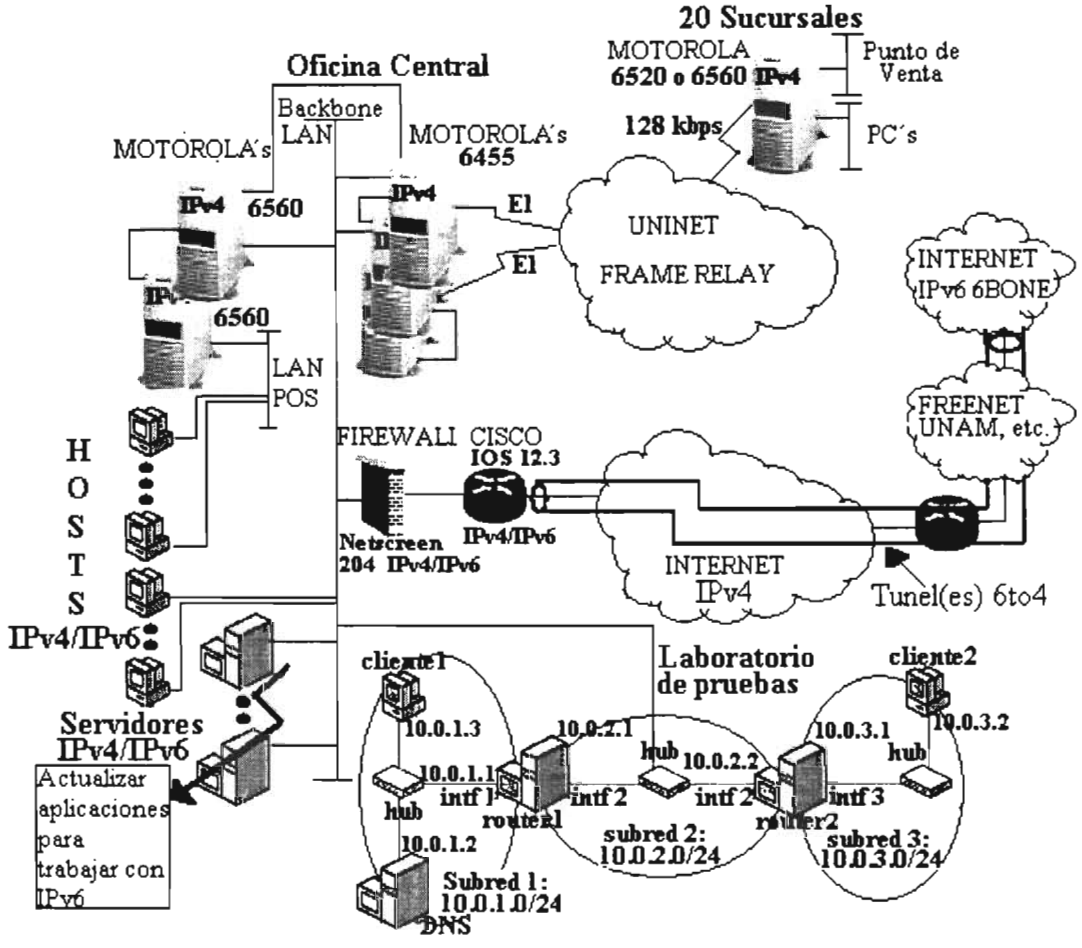


Fig. 4.14.1 Las aplicaciones se deben actualizar para que soporten la pila IPv6

Las aplicaciones nos deben permitir primeramente especificar el nodo destino usando su dirección IP o su nombre (mediante el uso del DNS para mapear el nombre en la dirección correspondiente. En ambos casos las aplicaciones deben ser modificadas para manejar las nuevas direcciones IPv6 de 128 bits. Estas direcciones pasan por los protocolos de transporte (TCP, UDP) los cuales también deben ser modificados.
Para que puedan hacer uso del protocolo IPv4 o protocolo IPv6 según el nodo destino con el que se quieran comunicar, se considera que seria mejor que también las aplicaciones mantengan una doble pila de IP para que puedan hacer uso de cualquiera de los dos protocolos.

Modificaciones a los sockets.
Los sockets deben ser redefinidos para manejar tanto IPv4 como IPv6, para que de esta forma se puedan actualizar tanto las aplicaciones escritas por usuarios finales como las pertenecientes a los sistemas operativos. Para cumplir esta tarea, las extensiones para sockets básicos (Basic Socket Interface Extensions for IPv6) proporcionan definiciones que los sistemas operativos derivados del Berkeley UNIX (4.x BSD) pueden usar y pueden ser implementadas a su vez en todos los otros sistemas operativos.

Una aplicación de Internet se puede desarrollar teniendo básicamente un sistema operativo que soporte los sockets de conexión como los de Berkeley y que se posean las interfaces de programación APIs para poder manipular dichos sockets.
El manejo de sockets se cumple desde el momento que se tiene soporte para IPv4, por su parte desde el momento que se tiene disponible un sistema operativo para IPv6, este sistema deberá incluir las APIs necesarias para desarrollar la aplicación.
Las APIs de IPv6 solo se diferencian de las de IPv4 en algunas opciones, no se diferencian mucho ya que esta fue una de las características que se tuvieron en cuenta cuando se diseño el protocolo, esta consideración se tuvo en cuenta para ayudar a que las aplicaciones no se vieran afectadas en cuanto a que deberían ser creadas nuevas aplicaciones, la características de similitudes entre IPv4 e IPv6 hace que solo se tengan que actualizar las aplicaciones, mas no crear nuevas aplicaciones.
El cambio de IPv4 a IPv6 afecta solamente a aplicaciones que usan sockets BSD en la parte de nombres y estructuras.
Actualmente muchas aplicaciones comerciales han sido actualizadas puesto que existe un gran numero de fabricantes que han realizado los cambios necesarios a sus aplicaciones, de hecho en Internet podemos encontrar un gran numero de aplicaciones listas para trabajar con IPv6.
En el caso de aplicaciones desarrolladas por las propias empresas una vez que se han migrado los servidores sobre los que se hospedan estas aplicaciones a nivel de capa de red, la aplicación puede ser actualizada modificando las interfaces de programación de aplicaciones APIs (Aplication Programing Interfaces) para que manejen los sockets de IPv6 también, para lo cual se tendrá que modificar ciertas estructuras y apuntadores o sockets de las aplicaciones.
Entre otras cosas algunos aspectos que se tienen que tener en cuenta para modificar las aplicaciones son:

- El tamaño de las direcciones, 32 bits para IPv4 y 128 bits para IPv6.
- Se debe tener en cuenta antes que nada, cuando se desarrollen nuevas aplicaciones que estas sean independientes del protocolo.
- Los cambios a las APIs de aplicaciones existentes deben tener en cuenta el tamaño de la dirección, la independencia de los protocolos, las dependencias sobre el tamaño del encabezado IP y sobre direcciones particulares.
- No todas las aplicaciones necesitan ser cambiadas ya que muchas no hablan a la red directamente.
- Aplicaciones que almacenan direcciones, ya que no se puede almacenar una dirección IPv6 de 128 bits en el espacio de una dirección de 32 bits.
- La modificación de las aplicaciones existentes solo se puede realizar si se cuenta con el código fuente.
- Se deben convertir las librerías de comunicaciones.
- La conversión a IPv6 debe ser sencilla.
- Se deben usar las mismas llamadas de sockets. Muchos de los sockets APIs no necesitan ser cambiados ya que fueron creados independientemente del protocolo y tienen apuntadores a sockets de direcciones (sockaddrs) como entrada salida.
- En el servidor se deben cambiar las funciones sockets, ajustar la función del registro para manejar direcciones IP más grandes e incrementar los datos de los miembros que guarden direcciones IP.

- En el cliente se deben cambiar las funciones socket, ajustar las funciones de registro, para poder manejar direcciones IP más grandes, se debe ajustar la función interfaz del teclado y de despliegue.
- Las APIs de resolución de nombres son las que más necesitan ser cambiadas.
- Sistema operativo donde se va a correr la aplicación.

La secuencia que ejecutan los códigos en un servidor es la siguiente:
1.- Se establece un socket por medio de la función (socket).
2.- Se realiza un ligamento de la dirección local al socket mediante la función (bind).
3.- Se escucha en un puerto mediante la función (listen).
4.- Se espera que se realicen conexiones mediante la función (accept).
5.- Se usan las funciones (read) y/o (write) si se usa TCP.
6.- Se usan las funciones (recvfrom) y/o (sendto) si se usa UDP.
La secuencia que ejecutan los códigos en un cliente es la siguiente:
1.- Se establece un socket por medio de la función (socket).
2.- Se conecta al servidor mediante la función (connect).
3.- Se usan las funciones (read) y/o (write) si se usa TCP.
4.- Se usan las funciones (recvfrom) y/o (sendto) si se usa UDP.
Debido a que IPv4 e IPv6 son muy parecidos, las funciones centrales de un socket como accept, connect y send no sufren cambios, IPv6 tiene cambios respecto a IPv4 en los siguientes 3 tipos de interfases:

- Estructura de los datos de dirección.
- Funciones para la traducción de nombre a dirección.
- Funciones de conversión de direcciones

Teniendo en cuenta estas consideraciones los cambios de nombres que se necesita realizar a una aplicación IPv4 para que funcione con IPv6 son:
1.- Cambios requeridos en la API a través de los sockets.
2.- Se necesitan nuevas estructuras de datos en las partes que muestren el tamaño de la dirección IP de la API.
3.- Se requieren cambios en las partes de la API que manipulen la dirección IP.

Nuevas macros.
Función socket
Los programas de aplicación usan la función socket ( ) para crear un descriptor de socket que representa el punto final de la comunicación. Los parámetros pasados a la función socket indican cual protocolo debe ser usado y cual es el formato de la dirección.
Una nueva macro llamada **AF_INET6** se ha definido en <sys/socket.h> para diferenciar la estructura de datos original sockaddr_in de la nueva estructura de datos **sockaddr_in6**. Adicionalmente otra macro nueva **PF_INET6** (Familia de protocolos) se ha definido y añadido a la librería regular de sockets y su valor es igual a **AF_INET6**.
Se debe reemplazar PF_INET por **PF_INET6** junto con la macro del protocolo de IPv6.
4.- Cambios en las funciones socket ( ) del núcleo:
Para crear una conexión TCP en IPv4 una llamada del siguiente tipo es usada:
s=socket(PF_INET, SOCK_STREAM, 0);
El valor PF_INET es el primer parámetro de la función socket para solicitar la creación de un socket en IPv4.

Si se quiere crear la misma conexión para IPv6 la función socket debe especificar **PF_INET6** como el primer parámetro:
s=socket(PF_INET6, SOCK_STREAM, 0);
Los cambios que se deberían implementar en estas funciones socket( ) del núcleo son:

- La longitud de la dirección.
- El espacio para nuevos campos en la cabecera.
- Mecanismos para poner nuevos valores de campo:

a) Para determinar la clase de trafico.
b) Opciones para la seguridad.

- Requerimientos de espacio y memoria.

Para garantizar la interoperabilidad y utilidad de las aplicaciones actuales la nueva API (Application Programming Interface) debe ser compatible con la antigua tanto a nivel fuente como binario. De esta forma la antigua aplicación puede crear cualquier combinación de comunicaciones TCP y UDP sobre IPv4 e IPv6.

Definición de la estructura de datos para direcciones IPv6.
5.- Cambios en las estructuras de datos para direcciones.

- Para IPv4 la familia de direcciones es AF_INET
- Se tiene una nueva familia de direcciones para IPv6 **AF_INET6** añadida a la librería regular de sockets. Se tiene que reemplazar AF_INET por **AF_INET6** junto con la macro de la familia de direcciones IPv6.
- Para IPv4: Estructura in_addr {Unsigned int s_addr}
- Para IPv6: La estructura de datos que contendrá una dirección IPv6 ha sido definida en el archivo <netinet/in.h> en la siguiente forma:

```
struct in6_addr {
        u_char s6_addr[16];   Estructura para la representación de las
};                            direcciones de la familia AF_INET6
```

Esta estructura de datos contiene un conjunto de 16 elementos cada uno de 8 bits de longitud, sin signo, que juntos forman la dirección IPv6 de 128 bits (16x8=128).

- Para IPv4: Estructura sockaddr {

```
u_short sa_family;  //Familia de direcciones
char sa_data[14]    //Datos de dirección
; }
```

El valor del campo sa_family indica que tipo de dirección tiene (IPv4, IPv6).

- La estructura in6_addr es usada para construir la nueva estructura **sockaddr_in6**, que contiene la dirección de un socket y es definida en la siguiente forma:

Para IPv6:

```
struct sockaddr_in6 {
    u_short sin6_family;      //AF_inet6
    u_short sin6_port;        // # puerto de la capa de transporte
    u_long sin6_flowinfo;     // Información de flujo IPv6
    struct in6_addr sin6_addr // Dirección IPv6
    u_long sin6_scope_id;}
```

Estructura que provee el espacio suficiente para soportar la estructura de 128 bits.

- Para IPv4: Estructura sockaddr_in {unsigned char sin_len
  Sa_familiy_t sin_family
  In_port_t sin_port
  Struct in_addr sin_addr}
- Para IPv6: Estructura **ssockaddr_in6 {uint8_t sin6_len**
  Sa_familiy_t sin6_family
  In_port_t sin6_port
  Struct in6_addr sin6_addr}
- ssockaddr_storage que es independiente del protocolo.
- Para IPv4 sin_port y sin_family
- Para IPv6 **sin6_port** y **sin6_family** la primera se usa para el numero de puerto de la capa de transporte y la segunda para la familia de direcciones **AF_INET6.**

Mapeo de nombres en direcciones y viceversa.

Para mapear nombres en direcciones y viceversa se adopto lo definido por el estandar POSIX 1003.1g (Protocol Independent Interfaces), es decir se adoptaron dos funciones diseñadas por el IEEE que son independientes del protocolo, las funciones **getaddrinfo** ( ) (para el mapeo de nombres en direcciones) y **getnameinfo** ( ) (para el mapeo de direcciones en nombres)

6.- Cambios en las funciones de traducción de nombre a dirección.

- En IPv4: gethosbyname () y gethosbyaddr ()
- En IPv6: getipnodebyname () getipnodebyaddr ()
- Se tienen dos nuevas funciones para IPv4 e IPv6 que son independientes del protocolo, es decir trabajan tanto en IPv4 como en IPv6:
  - **getaddrinfo** ( ). Obtiene las direcciones asociadas a un nombre hallando las direcciones y/o números de puerto que corresponden a un nombre de host y servicio dados.
  - **getnameinfo** ( ). Realiza el mapeo inverso, es decir encuentra el nombre de host y/o nombre de servicio que corresponde a una dirección o numero de puerto dado.

Modificaciones al servicio de nombres de dominio (DNS)

Las llamadas a las funciones de mapeo de nombres en direcciones y viceversa no pueden ser ejecutadas si el DNS no es actualizado, permitiéndole almacenar direcciones IPv6.

- Para el mapeo de nombres en direcciones un nuevo tipo de registro **AAAA** ha sido agregado, derivado del registro A de IPv4 usado para almacenar direcciones IPv4 y como las direcciones IPv6 son cuatro veces más grandes que las direcciones IPv4, se decidió usar cuatro A´s. En IPv4 este mapeo se realiza en un registro o archivos de configuración de la siguiente forma:

Cliente1.labpruebas.mx IN A 192.0.0.24

Es la misma operación para el mapeo de nombres en direcciones IPv6, pero con registros **AAAA**:

Cliente1.labpruebas.mx IN AAAA fec0:0:1:2:20d:9dff:fe55:2f41

- Para el mapeo de direcciones en nombres, IPv4 usa un registro PTR:

24.0.0.192.IN-ADDR.ARPA PTR cliente1.labpruebas.mx

Como el dominio ARPA es obsoleto se definió un dominio **IP6** de segunda capa bajo el dominio de primera capa INT, así el mapeo de direcciones a nombres en IPv6 es:
1.4.f.2.5.5.e.f.f.f.d.9.d.0.2.0.2.0.0.0.1.0.0.0.0.0.0.0.0.c.e.f.IP6.INT PTR cliente1.labpruebas. mx

Mapeo de direcciones binarias en direcciones ASCII y viceversa
Cuando se necesita interactuar con los seres humanos, se necesita traducir el formato de una dirección numérica en un formato textual o viceversa, para esto se han definido dos nuevas librerías de funciones:
inet_pton ( ) Función que realiza el mapeo de un formato textual a un formato numérico.
inet_ntop ( ) Función que realiza el mapeo de un formato numérico a un formato textual.
7.- Cambios en las funciones de conversión de direcciones entre ASCII (binario) y la forma de red de las direcciones (cadena)

- En IPv4: de binario a cadena = inet_ntoa ()
- En IPv6 e IPv4: de binario a cadena **inet_ntop** (). Reemplazar junto con la función de traducción de direcciones IPv6.
- En IPv4: de cadena a binario = inet_aton () e inet_addr
- En IPv6 e IPv4: de cadena a binario = **inet_pton** ( ). Reemplazar junto con la función de traducción de direcciones IPv6.

A continuación se tiene un ejemplo de cómo usar un socket AF_INET6 con soporte para comunicaciones IPv6 e IPv4:

- Para que el socket permita las comunicaciones con IPv6 debe crearse un socket AF_INET6, este socket sera usado por la estructura sockaddr_in6 que contiene una dirección IPv6.
- Para que el socket permita las comunicaciones con IPv4 debe crearse un socket AF_INET6, este socket será usado por la estructura sockaddr_in6 que contiene una dirección IPv4 mapeada a IPv6 del tipo ::ffff:201.134.200.18.

Las dependencias sobre el tamaño del encabezado deben ser tomadas en cuenta para programas que calculan el tamaño de la carga útil del datagrama calculando el MTU (tamaño del encabezado UDP+tamaño del encabezado IP) necesitan saber que el tamaño del encabezado IP ha cambiado.
Estos son algunos de los cambios más importantes requeridos en las APIs para migrar las aplicaciones de IPv4 a IPv6, se han desarrollado algunas herramientas para apoyar esta actualización, estas herramientas ayudan a identificar las líneas de código fuente que requieren cambiarse o actualizarse.
Para escribir una aplicación IPv6 para un sistema operativo Windows los elementos básicos requeridos son:

- Tener disponible la plataforma SDK 2000, la cual esta disponible en http:://msdn.microsoft.com
- Software de programación Visual C++ 6.0.
- El protocolo IPv6 de Microsoft, el cual contiene los archivos y librerías de las APIs.

Algunas recomendaciones que se han definido para el desarrollo de las aplicaciones son:

- Desarrollar las aplicaciones independientes de la familia de direcciones ya que es la mejor manera de conversión para tener la mayor portabilidad posible.

- Esconder el código dependiente del protocolo mediante las funciones: getnameinfo () getaddrinfo ()
- Habilitar la aplicación para usar las características de IPv6.

En el caso de Microsoft por ejemplo, plataforma base de la red propuesta, los equipos ya soportan la pila IPv6, pero además se puede decir que algunas aplicaciones ya soportan el uso de la pila IPv4 o IPv6, ya que con las pruebas realizadas en el laboratorio conectado a la red, pudimos comprobar por ejemplo que las utilerías de diagnostico como ping, pathping, tracert soportan ya sea IPv4 o IPv6, por ejemplo con el comando ping se le puede indicar al equipo que haga la petición de esta prueba con una dirección IPv4 o IPv6, es decir:

- ping 192.0.0.4
- ping fe80::20b:cdff:fea9:528b%5

Como vemos el protocolo ICMP aunque puede usar directamente la utilería ping6 para manejar directamente las direcciones IPv6 con la misma utilería ping puede probar la conectividad a direcciones IPv4 o direcciones IPv6 por lo que ICMP ya soporta el uso de IPv4 o IPv6, ya que lo mismo sucede con un tracert o pathping.

También pudimos ver que las aplicaciones en Microsoft para transferencia de archivos con ftp, la navegación web y la conexión remota con telnet ya soportan también ambas pilas puesto que se pueden usar cualquiera de ellas para realizar su función con IPv4 e IPv6.

Aunque en el caso del ftp y http no estan del todo actualizadas. En el caso del ftp, la parte del cliente ftp no tiene ningún problema para manejar IPv6 pero la parte del servidor ftp mandaba error cuando se quería hacer la conexión a direcciones IPv6.

Las pruebas hechas con ftp como al igual que todas las demas pruebas se hicieron localmente con los equipos conectados en la red y más particularmente en el laboratorio, y se probaron hacia sitios IPv6 cuando se realizo la conexión a Internet.

Cuando se hicieron las pruebas localmente ya sea con direcciones link local, site local, isatap, v4-compatibles o 2002, se intentaron hacer conexiones con estas direcciones via ftp al servidor DNS que tenia instalado windows server 2003, conexiones que siempre mandaban error, aunque con direcciones IPv4 la conexión al DNS por ftp no tenia ningún problema.

Cuando se realizo la conexión a Internet se realizaron las mismas pruebas con sitios IPv6, es decir, ping, tracert, telnet, ftp, http. Cuando se encontró un sitio IPv6 con el servicio de FTP habilitado se realizo la conexión exitosamente sin problema alguno. Con esto podemos decir que la aplicación cliente ftp de Microsoft se encuentra actualizada para manejar IPv6 también, mas no la aplicación servidor ftp.

Por otro lado cuando se realizaron las pruebas con http, pudimos darnos cuenta que la aplicación de navegación Web de Microsoft no esta actualizada del todo, ya que aunque si permite navegar en sitios IPv6 por nombre de dominio, no entiende que se le indique la dirección destino IPv6 en la barra de direcciones URL en el formato que se definió cuando se diseño el protocolo IPv6, http://[_fe80::20b:cdff:fea9:528b%5]:80, es decir la dirección IPv6 entre corchetes, sin embargo si realiza la conexión al sitio IPv6 por nombre de dominio como http://www.ipv6.unam.mx, el detalle aquí esta en que el navegador hace el dialogo con el servidor DNS para conocer tanto las direcciones IPv6 como IPv4 del sitio, lo que puede prestarse a confusión y pensar que se realizo la conexión con la dirección IPv6 y probablemente el navegador tomo la dirección IPv4.

Aunque pudimos comprobar que si puede hacer la conexión http con la dirección IPv6, puesto que en el caso de la dirección de Microsoft http://www.ipv6.microsoft.com la

dirección que corresponde a esta URL es únicamente una dirección IPv6 y se conecta puesto que recibimos una respuesta (Thanks by dropping) del sitio. Por lo que la aplicación Internet Explorer de Microsoft necesitaría nada mas ser actualizada para que maneje las direcciones IPv6 entre corchetes.
Se hace mención de estos detalles que sirven como indicadores de que ya muchos fabricantes efectivamente han actualizado tanto su plataforma como sus aplicaciones para manejar el protocolo IPv6.

4.15 Instalación de servidores adicionales como DNS y DHCP6

IPv6 tiene 2 grandes características, una es la longitud de 128 bits de las direcciones y otra es la de autoconfiguración.
En la practica la longitud de direcciones IPv6 tan largas hará que su uso por los usuarios finales sea imposible. Los usuarios trabajaran con IPv6 solamente usando nombres y esos nombres serán convertidos en nombres por servidores DNS.
Si anteriormente conectamos a un sitio o host con una dirección IPv4 no era muy común si no se conocía la dirección IP, con IPv6 será difícil tratar de hacer conexiones, búsquedas o pruebas a direcciones IPv6, por ejemplo no se le puede decir a un usuario x que realice un telnet a la dirección IPv6 en formato hexadecimal del servidor w, para cualquiera será muy difícil acordarse de una dirección tan larga y al usuario le seria muy difícil teclear una dirección tan larga, por lo que seria más fácil y practico pedirle que realice un telnet a la dirección nominaipv6.productosparaelhogar.com por ejemplo.
Será necesario manejar servidores DNS que tengan la capacidad de manejar registros para direcciones IPv6, como son los registros AAAA, con IPv4 muchas empresas solamente manejaban los servidores DNS para comunicación hacia el Internet, con el uso de IPv6 desde mi punto de vista será necesario instalar un servidor DNS en las redes locales para el manejo de direcciones internas de la red por medio de nombres, lo cual hará más fácil la interacción con estas direcciones IPv6 haciendo más fácil y transparente la migración para el usuario. Es decir con IPv6 se tendrá que cambiar la forma de indicar a las aplicaciones a donde nos queremos comunicar, para lo cual ahora deberemos manejar mas nombres, que direcciones. Es como extender un poco el ambiente de Internet hacia dentro de nuestras redes con el manejo de la resolución de nombres en direcciones IPv6.
El DNS debe ser configurado con un componente que soporte IPv6 y con una librería de resolución que maneje ambos tipos de registros IPv4 e IPv6.
Para hosts con doble pila IPv6/IPv4 el DNS seleccionado debe proporcionar librerías que manejen registros de recursos AAAA IPv6 y registros A IPv4 y deben ser capaces de manejar los casos donde una petición localiza ambos registros IPv4 e IPv6. En este caso la librería de resolución DNS puede regresar la dirección IPv6, la dirección IPv4 o ambas. La aplicación después usa el protocolo IPv6 o el protocolo IPv4 o hace una elección entre los dos basándose en el trafico IP y en los requerimientos particulares de la comunicación.
El DNS debería ejecutar o tener capacidades equivalentes a la versión 9 de Berkeley Internet Name Domain (BIND). Esta versión proporciona una implementación de los principales componentes del DNS (DNS server, librería de resolución y herramientas de verificación) para IPv6.

Con las pruebas realizadas con el laboratorio conectado a nuestra red pudimos comprobar que los servidores DNS actualmente instalados en Internet ya soportan tanto el manejo de registros típicos de IPv4 y los de IPv6 AAAA, esto lo comprobamos, ya que se realizaron pruebas desde nuestro laboratorio hacia el Internet haciendo un encapsulamiento y usando el router relay de Microsoft para tener comunicación a sitios IPv6 buscándolos por sus nombres y pudimos constatar que los servidores que usamos normalmente para comunicarnos a sitios IPv4 ya cuentan también con la capacidad de resolver nombres de sitios en direcciones IPv6, con la conexión del laboratorio a Internet se hicieron pruebas con ping, tracert, telnet, ftp, http, a los sitios indicando los nombres de dominio teniendo como servidores DNS los que usualmente manejamos para Internet y estos resolvían sin ningún problema los nombres de dominio en direcciones IPv6.
En nuestro servidor DNS con Windows Server 2003 instalado en el laboratorio de pruebas se configuraron registros AAAA para los diferentes tipos de direcciones IPv6 (link local, site local, isatap, 3FFFE, 6to4) y no se encontró problema alguno para comunicarse entre nodos por medio de los nombres resolviendo a direcciones IPv6.
Por lo anterior, la instalación de un servidor DNS en las redes locales será muy necesaria para facilidad y comodidad en el manejo de las largas direcciones IPv6.

Por otro lado los administradores de red se enfrentaran con las longitudes de las direcciones y deberán adquirir las herramientas de soporte necesarias para la configuración de red, la configuración de direcciones IPv6 no directamente sobre hosts sino sobre servidores DHCP será común y así los hosts cuando son reiniciados o encendidos interactúan con servidores DHCP para configurar sus direcciones y sus prefijos (subredes).
Si queremos usar la característica de autoconfiguración de direcciones de IPv6 podríamos usar la autoconfiguración por anunciamiento de prefijo por parte de los routers con lo cual los nodos pueden tomar dicho prefijo y agregarlo a su identificador de interfaz en formato EUI-64 para formar sus direcciones, o podríamos optar por instalar un servidor DHCP para que después de la negociación con el nodo solicitante asigne una dirección valida al nodo, esta opción del servidor DHCP podría ser una opción para que se use durante el dialogo de negociación de dirección algún sistema de autentificación y validación asignado a los usuarios permitidos para que solo estos puedan obtener una dirección ya que con la opción por anunciamiento de router cualquier gente no autorizada podría conectarse a la red y obtener una dirección de nuestra red con lo cual podrían permitirse intromisiones no deseadas en la red. En base a esto se puede instalar opcionalmente un servidor DHCP6.

En la practica los servidores DHCP son bases de datos que contienen relaciones entre direcciones de enlace (direcciones MAC) y direcciones IPv6, mientras que los servidores DNS contienen relaciones entre direcciones IPv6 y nombres. Como ambos tipos de servidores son prácticamente obligatorios con IPv6 y por que ambos comparten direcciones IPv6, soluciones integradas de servidores DHCP y DNS basadas en una base de datos común seria preferida.
Este punto seria opcional ya que no es obligatorio la instalación de estos servidores, esto es mas que nada para facilidad de manejo de las direcciones IPv6, asi como para implementación de probables mecanismos de seguridad en la autoconfiguración de direcciones IPv6, una vez realizado esto nuestro diagrama quedaría como muestra la Fig. 4.15.1:

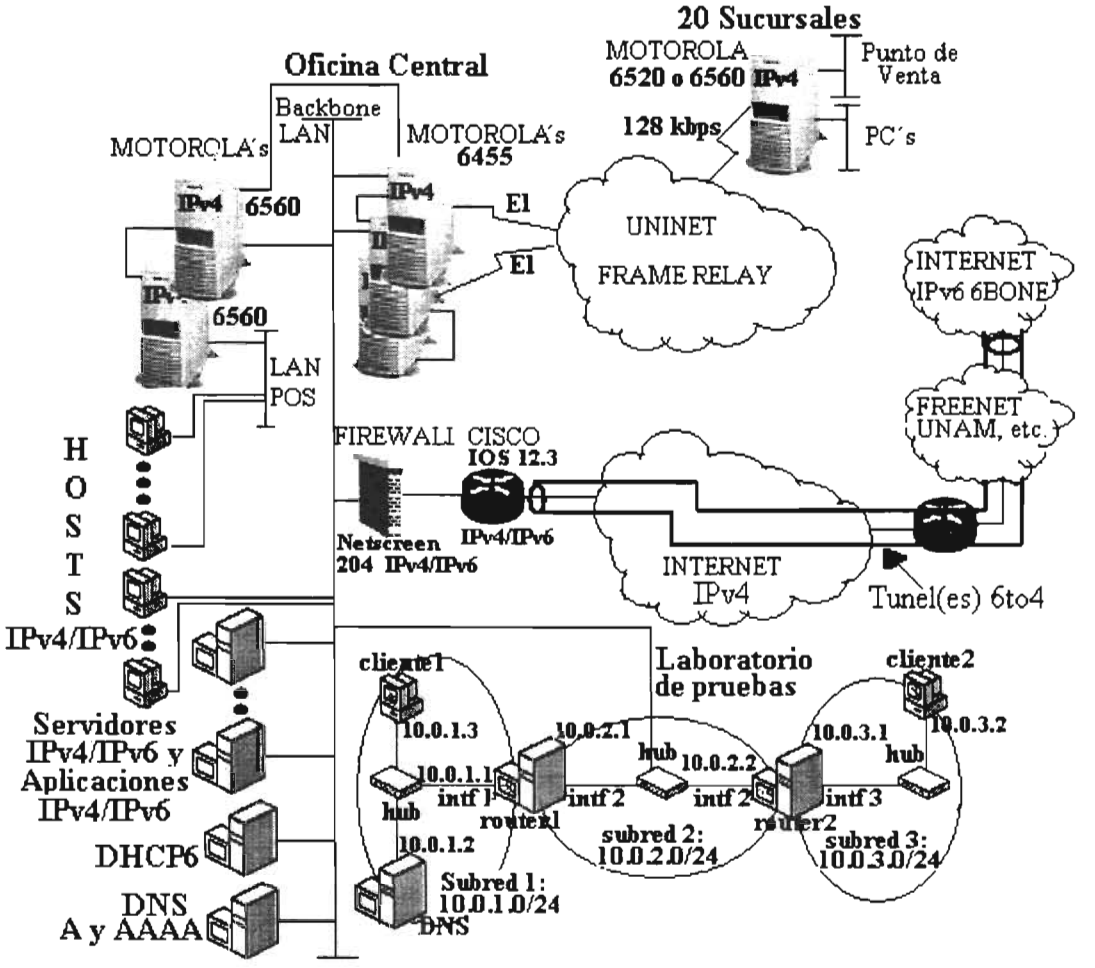


Fig. 4.15.1 Instalación opcional de servidores DNS y DCHP6 en la red local

4.16 Actualización de ruteadores que conforman el backbone de la red interna.

Los ruteadores se dejaron al final por que son la espina dorsal de la red y una de las partes mas criticas de la red ya que estos equipos además de manejar los datos manejan la voz y por que la plataforma de ruteo interna de la red podría seguir funcionando con IPv4 el tiempo que sea necesario, o durante el tiempo de vida útil de los equipos actuales, ya que con los equipos hosts y servidores actualizados con IPv4/IPv6, la comunicación con IPv4 actual seguirá funcionando igual y con las direcciones IPv6 autoconfiguradas al mismo tiempo se tiene la conectividad al Internet IPv6 por medio del router o equipo que maneje el prefijo ya sea delegado por un nodo pTLA o nTLA o con el prefijo automático.
Dependiendo de una de las dos siguiente necesidades:

1) Que únicamente se tenga conectividad al backbone de IPv6
2) Que además de la conectividad al backbone de IPv6 la red local internamente maneje el ruteo completo de IPv6.

Para el primer punto con lo realizado hasta aquí se puede cumplir, es decir con los equipos hosts y servidores manejando la doble pila y la conexión establecida al backbone de IPv6, mediante un túnel, además de los puntos anteriores implementados la conectividad a la red IPv6 se puede realizar, desde el momento en que un nuevo equipo con el protocolo IPv6 habilitado se conecte al mismo segmento del router o gateway IPv6 recibirá el anunciamiento del prefijo por parte del router y se autoconfigurará y tendrá acceso al 6BONE, al mismo tiempo toda la red puede continuar con su funcionamiento normal con IPv4 por medio de la pila IPv4 ya que el hecho de que a un host o servidor se le habilite la pila de IPv6, la parte de IPv4 sigue funcionando igual.
Para el punto 2 estamos hablando prácticamente de una red con IPv6 nativo, este es el objetivo deseado al que deberá llegarse en algún momento es decir que tanto la conexión a Internet sea con enlaces IPv6 nativos como toda la comunicación de capa de red en una red local sea también con IPv6.
En el caso de nuestra red se ha dejado al final la parte de ruteadores que componen el backbone de ruteo de la red debido a que estos equipos son de la marca Motorola modelos 6560 y 6520, estos equipos son de función critica en la red de comunicaciones ya que manejan voz y datos todo encapsulado en frame relay para realizar la comunicación hacia las sucursales. Estos equipos no solamente rutean trafico de datos de IP por lo que tiene una cierta configuración un tanto compleja tanto en hardware como en software para el manejo de voz y datos, ya que además de manejar los puertos ethernet para conexión a la red lan, manejan puertos seriales V24 y V35, asi como tarjetas E1.
Después de consultar con los distribuidores directos del fabricante de este tipo de equipos, a la fecha el fabricante no tiene pensado desarrollar alguna versión de software para manejar IPv6, por lo que no se puede pensar en realizar una simple actualización de software en este tipo de equipos.
Por lo anterior lo que se propone es mantener la infraestructura de ruteadores motorola para que continúen manejando la parte de encapsulamiento en frame relay para la voz y también para los datos de IPv4.
Por lo que una opción que se propone es agregar un ruteador Cisco con doble pila IPv4/IPv6 que se encargara de manejar directamente el trafico IPv6 entre los hosts de la oficina central y los de las sucursales, este router tal vez podría desempeñar una función de router ISATAP (Protocolo de túnel automático Intrasite) para manejar el trafico entre hosts IPv6 a través de la Intranet IPv4 manteniendo la comunicación a través de los equipos Motorola por medio del encapsulamiento IPv4 y con los hosts IPv4/IPv6 y servidores IPv4/IPv6.
Es decir el proceso de ruteo prácticamente ya recaería solamente sobre el nuevo router Cisco instalado, dejándose los routers Motorola para manejar la voz y las conexiones WAN entre sucursales y oficina central.
De esta manera el diagrama quedaría de la siguiente forma, Fig. 4.16.1:

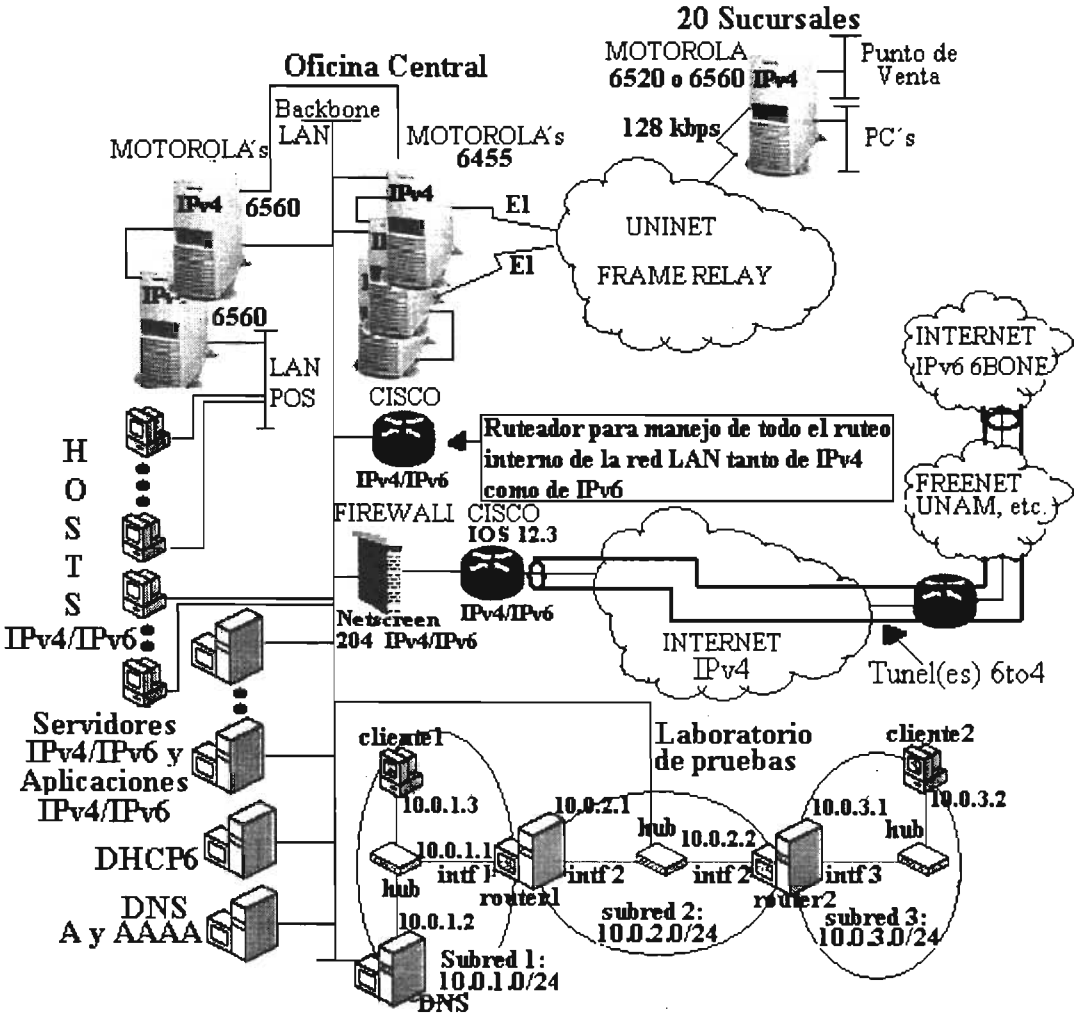


Fig. 4.16.1 Actualización de equipos de ruteo internos

Con el laboratorio de pruebas se implemento un esquema en el que la subred 1 del laboratorio tenia conectividad IPv6 nativa y el resto del laboratorio, es decir los segmentos 2 y 3 tenían conectividad IPv4 únicamente, es decir formaban una Intranet con IPv4 únicamente, el router que estaba entre la subred IPv6 y la Intranet, o sea el router 1 se configuro como router ISATAP y se realizaron las pruebas correspondientes para verificar que se tuviera comunicación entre los hosts de l subred IPv6 y los de la Intranet IPv4, las pruebas funcionaban perfectamente ya que el router 1 o ISATAP encapsulaba el trafico IPv6 hacia la Intranet con un encabezado IPv4 para que circulara libremente por la Intranet y el trafico que provenía de la Intranet tenia como dirección fuente la del router ISATAP por lo que también era posible la comunicación desde la Intranet IPv4 a la subred IPv6.

La otra opción es cambiar la plataforma de ruteo por otra marca, en este caso la opción más viable es por la marca Cisco, ya que Cisco a parte de ser una de las empresas lideres en el ruteo de IP es una de las marcas que más han desarrollado su soporte para IPv6.

Hasta hace poco se había obtenido un presupuesto por parte de Cisco para cambiar la plataforma Motorola completamente por Cisco cumpliendo con todas las características, y comparados con una actualización de los mismos equipos por otros de la misma marca pero de modelos más actuales la oferta de Cisco era más barata.

De cualquier manera la opción de cambiar la plataforma de ruteo no se descarta por lo que en el diagrama 4.16.2 tenemos la red local con la actualización de la plataforma de ruteo a Cisco.

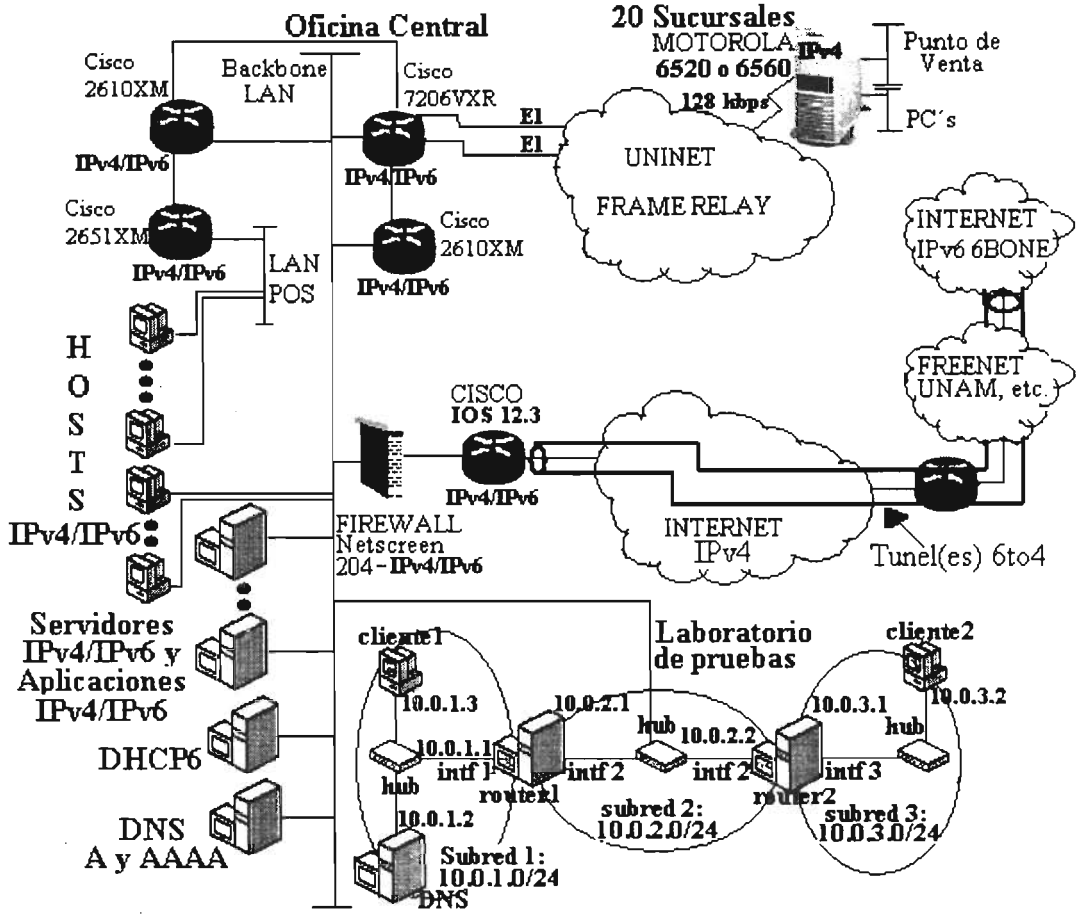


Fig. 4.16.2 Actualización de la plataforma de ruteo Motorola a Cisco

Como podemos ver en la figura 4.16.2 se sigue manteniendo el mismo esquema, los modelos de Cisco mostrados fueron cotizados con el proveedor de tal manera que cumplieran con las características que tenían los equipos motorola, es decir, se cotizaron con puertos ethernet, puertos seriales sincronos y asíncronos, interfaces RS-232, V-35 y G703.

En el caso de las sucursales, podríamos aplicar el mismo procedimiento general propuesto y en el punto de actualización de router, ni se puede actualizar el router Motorola ni creo que seria buena opción instalarle un router cisco adicional para manejar IPv6, ya que al fin y al cabo la comunicación hacia la oficina central que es lo que más interesa en las sucursales se hará a través de IPv4, sin embargo la actualización de todos los demás elementos de la red en las sucursales puede ser implementada sin ningún problema conforme al procedimiento general. De cualquier manera aplicando el procedimiento general se tendrían que actualizar los hosts y servidores a IPv6 y el ruteador tendría que ser cambiado por un cisco, esto se muestra en la fig. 4.16.3.

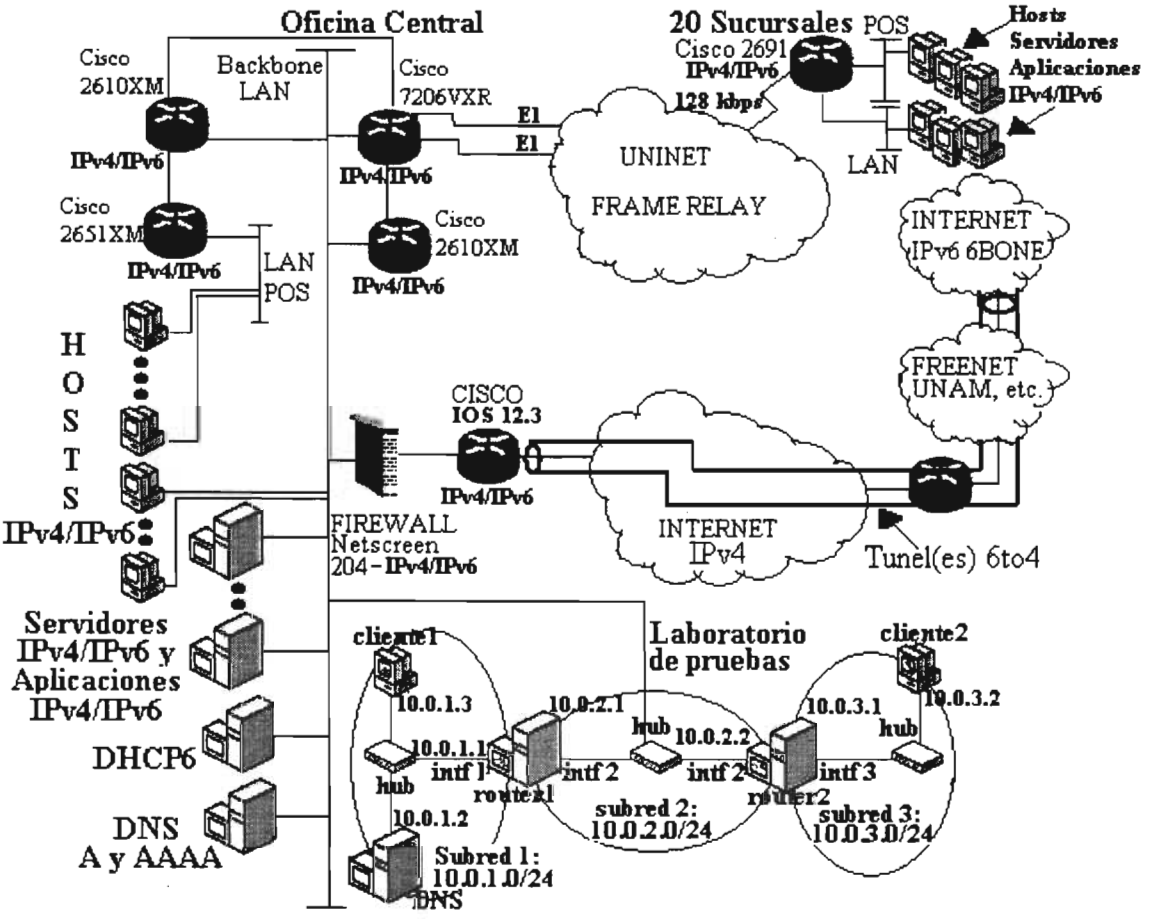


Fig. 4.16.3 Actualización de las sucursales

La actualización de las sucursales seguiría el mismo procedimiento, en este caso el equipo de ruteo se tiene que cambiar por un Cisco que cumple también con las características de los routers Motorola, con tarjetas de voz, puertos ethernet y seriales.

Estos son los pasos generales que proponemos para implementar la migración de la red, con los cuales se intenta manejar tanto IPv6 como IPV4 y que la red no pierda su estructura actual que es una de las condiciones de la migración, no afectar el funcionamiento y por lo tanto no modificar nuestra red, asimismo se ha tratado de hacer que los costos implicados para realizar esta migración sean mínimos.
Con el laboratorio de pruebas implementado y con las diferentes pruebas realizadas, así como con los resultados capturados de los paquetes IPv6, entre otras cosas tratamos de comprobar el cumplimiento de la teoría con la practica por lo que se elaboro en base a esos resultados una tabla que indica si se cumplen las características de IPv6:

Característica de IPv6	Coinciden teoría y practica
Tamaño del encabezado de 40 bytes	SI
Encabezado más eficiente (menos campos)	SI
Permite encabezados opcionales	SI
Identifica el encabezado AH=51	SI
Identifica el protocolo IPv6=41	SI
Identifica el encabezado ESP=50	SI
No realiza segmentación	SI
Administración de flujos de datagramas con etiquetas de flujo	SI
Elimina control de errores en la cabecera	SI
El tipo de contenido manejado en Ethernet para IPv6 es 86DD	SI
Anunciamiento de prefijos por parte de los routers	SI
Autoconfiguración de direcciones link local fe80	SI
Autoconfiguración de direcciones site local fec0	SI
Autoconfiguración de túnel fe80::5efe:w.x.y.z	SI
Autoconfiguración de direcciones v4-compatibles ::w.x.y.z	SI
Autoconfiguración de direcciones 6to4 temporales 3FFE	SI
Autoconfiguración de direcciones 6to4 globales 2002	SI
Convivencia de IPv4 con IPv6 mediante túneles de IPv6 dentro de IPv4	SI
Encapsulamiento de IPv6 dentro de IPv6	SI
Autoconfiguración de direcciones unicast globales mediante el uso del identificador de la dirección física EUI-64	SI
Permite seguridad de encabezado y de confidencialidad AH y ESP	SI

Asimismo con las utilerías, aplicaciones o herramientas que se usaron para realizar las pruebas una tabla de resultados:

Tipos de direcciones	Funcionamiento de la prueba				
	PING	TRACERT	PATHPING	TELNET	FTP
Link local (FE80)	OK	OK	OK	OK	NO
Site local (FEC0)	OK	OK	OK	OK	NO
ISATAP (FE80::5EFE:w.x.y.z)	OK	OK	OK	OK	NO
Temporales (3FFE)	OK	OK	OK	OK	NO
v4compatibles (::w.x.y.z)	OK	OK	OK	OK	NO
Globales 6to4 (2002)	OK	OK	OK	OK	NO

Tipos de direcciones	Funcionamiento de la prueba		
	http	Seguridad	Resolución de nombres en direcciones IPv6
Link local (FE80)	No se probo	OK	OK
Site local (FEC0)	No se probo	OK	OK
ISATAP (FE80::5EFE:w.x.y.z)	No se probo	No se probo	No se probo
Temporales (3FFE)	No se probo	No se probo	OK
v4-compatibles (::w.x.y.z)	No se probo	No se probo	No se probo
Globales 6to4 (2002)	OK	OK	OK

Las pruebas indicadas como "no se probo", aunque no se probaron deben de funcionar, puesto que se probaron con algún otro tipo de dirección, deben funcionar con todas las demás ya que solamente cambia el formato o prefijo de la dirección.

De las pruebas realizadas en los diferentes esquemas con direcciones IPv6 globales 6to4 (2002) podemos concluir que no se encontró ningún problema para el uso de estas direcciones en ambientes de producción ya que trabajan perfectamente con las direcciones IPv4 gracias al encapsulamiento que realizan, las pruebas hechas con IPv6 para hacer ping, tracert, pathping, telnet, ftp y http funcionaron sin ningún problema ya sea usándolas en una red local con direcciones IPv6 únicamente, para conectar redes IPv6 con redes IPv4 o conectando dos redes locales a través del Internet para hacer circular el trafico de IPv6 por redes que manejan únicamente IPv4. Asimismo se pudo comprobar que los servidores no representan problema alguno para resolver nombres de hosts en direcciones IPv6. Las pruebas con seguridad usando los protocolos ESP y AH también fueron exitosas dentro de los alcances o limitaciones que todavía tiene el sistema operativo para aplicar seguridad en la pila de IPv6.

Un detalle que se tuvo durante las pruebas fue que con el ftp no se pudieron hacer conexiones aun cuando el servicio de FTP estaba levantado en los hosts destino, puesto que se probo el servicio de FTP con IPv4 y si se podía realizar la conexión, sin embargo el dialogo entre maquinas con direcciones IPv6 para entablar la conexión ftp se realiza pero se rechaza la conexión al final, lo cual pudiera ser algún detalle que se tenga que corregir en las interfaces de aplicación APIs del servicio de ftp para que permita realizar o concretar la

conexión con direcciones IPv6, o para que reconozca direcciones en el formato de IPv6 como lo hacen perfectamente el PING, TRACERT, PATHPING, TELNET, y servidores DNS. El servicio de FTP que se uso para las pruebas fue el servicio FTP que tiene por default el sistema operativo de Microsoft Windows Server 2003.
Las pruebas con ftp no funcionaron ya que nunca se pudo establecer una conexión con ftp entre maquinas que se encontraban dentro del laboratorio, tanto el servidor como el cliente ftp que se uso para estas pruebas eran los de Microsoft, esos mismo intentos de conexión por ftp entre los nodos con IPv6 se checaba con IPv4 y no tenia ningún problema, por lo que tanto el servidor como el cliente estaban levantados. Cuando se realizo la conexión a un sitio IPv6 en Internet que si permitía la conexión por ftp se pudo realizar la conexión, por lo que deducimos que el cliente ftp de Microsoft no presenta problema alguno, siendo el del problema el servidor ftp de Microsoft, el cual probablemente no tiene actualizadas sus APIs para manejar la pila de IPv6.
El caso de http se probo mas que nada hacia sitios IPv6 de Internet, ya que en el laboratorio no se pudo instalar por falta de tiempo un servidor web, pudimos observar que el funcionamiento del protocolo http en si no presenta problema alguno, en lo que si presento un detalle fue el navegador utilizado en este caso el Internet Explorer de Microsoft, el navegador podía trabajar con IPv6 siempre y cuando se le indique el nombre del sitio IPv6 con lo cual el se encarga de hacer la petición al DNS para conocer la dirección IPv6 del sitio y realizar la conexión, pero cuando se le indica en la barra de direcciones o URL la dirección del sitio en forma de dirección IPv6 encerrada entre brackets como se estableció para el manejo de direcciones IPv6 en navegadores, es decir se encontró que el navegador de Internet Explorer no acepta o no maneja las direcciones IPv6 explícitamente, ya que según se estableció cuando se definió IPv6 que:

- Las direcciones IPv6 en una dirección URL se deben encerrar entre paréntesis cuadrados ([ ]) en la forma:

http://[::FFFF:129.144.52.38]:80/index.html

el browser no entiende el formato de estas direcciones y manda error, sin embargo si se teclea el nombre del host, el browser pregunta al servidor DNS las direcciones IPv4 e IPv6 correspondientes al nombre, el DNS le devuelve ambas direcciones, IPv4 e IPv6 y de esta forma se puede realizar la conexión por http, por lo que deducimos que el navegador no esta del todo actualizado ya que por un lado si permite la conexión por nombre del nodo y maneja la dirección IPv6 regresada por el servidor DNS, pero por otro no entiende la dirección IPv6 directamente en formato de 8 campos hexadecimales separados por dos puntos, el que solamente se puedan realizar conexiones por resolución de nombres pudiera deberse a que falte modificar las interfaces API en el Internet Explorer para que entienda, maneje y acepte el formato de las direcciones IPv6.
El funcionamiento de IPv6 se comprobó con las pruebas del laboratorio conectado al ambiente real de la red local y con conectividad a Internet por lo que podemos afirmar que:

- Primeramente la teoría se cumple exactamente en la practica del funcionamiento de IPv6.
- El funcionamiento y establecimiento de IPv6 es ya una realidad.
- Su uso actual en Internet es realmente bastante extenso, ya que podemos encontrara sitios con IPv6 nativo, servidores DNS instalados en Internet ya con la capacidad de resolver nombres de sitios a direcciones IPv6, routers relay en funcionamiento que permiten tener conectividad hacia sitios IPv6 pasando por Internet.

- Existe actualmente una amplia variedad de aplicaciones ya probadas que funcionan con IPv6.
- Así mismo los sistemas operativos de PCs y servidores en su gran mayoría han sido actualizados en sus más recientes versiones por los fabricantes para el manejo de IPv6.
- Una gran cantidad de fabricantes de equipo de interconexión esta desarrollando y liberando sus equipos con la capacidad de manejo de IPv6, incluso un gran numero de ellos ha liberado versiones para prueba y para producción.
- La coexistencia entre ambos protocolos funciona perfectamente ya sea usando túneles de IPv6 a través de IPv4, túneles con otras técnicas como túneles isatap 6to4, con el uso de direcciones compatibles, etc. Durante las pruebas realizadas el funcionamiento de las diferentes técnicas para hacer interactuar redes IPv6 con redes IPv4 y viceversa no presentaron problema alguno, se comunico el laboratorio de pruebas conectado internamente a la red local por medio del acceso a Internet para poder llegar a sitios y hosts IPv6, resultando las pruebas satisfactorias.
- Se comprobó también que los equipos que en un momento dado no puedan ser migrados no tendrán problemas para interactuar con los equipos que manejen IPv6 a través de los túneles de Ipv6 sobre IPv4, entre las pruebas implementadas en nuestro laboratorio se implementaron varios esquemas para comunicar redes IPv6 a través de intranets IPv4 por lo que el trafico de IPv6 circulaba encapsulado por los equipos que solamente manejan IPv4 y en ningún momento estos presentaron problema alguno para el transito de este tipo de trafico. Asimismo hacia Internet se empleo también el método de túnel IPv6 sobre IPv4 para llegar a sitios IPv6 pasando por nuestro Cisco aun sin actualizar el IOS y por los equipos de nuestro ISP sin tener ningún problema para comunicar nuestro laboratorio IPv4/IPv6 con sitios del 6BONE

La propuesta realizada busca tener un funcionamiento de doble pila IPv4 e IPv6, ya que es un hecho que debido a la gran cantidad de infraestructura de IPv4 instalada la migración a IPv6 tendrá que ser forzosamente a través del uso simultaneo de los dos protocolos, hasta que se llegue el momento en que toda la red e infraestructura maneje IPv6 para poder deshabilitar IPv4 lo cual no sucederá durante mucho tiempo, ya que es un hecho que para manejar IPv6 nativo sin el uso de IPv4 se tendría que instalar prácticamente una red nueva como lo han hecho las empresas e instituciones que han estado probando el funcionamiento de IPv6, esta red tendría que ser paralela a las conexiones actuales de Internet lo que provocaría gastos adicionales y mayor complejidad en la comunicación, en el caso de 6BONE la red IPv6 para pruebas presenta este caso donde se tuvo que instalar una red totalmente nueva para las pruebas, la cual internamente maneja el IPv6 puro, pero para comunicarse al exterior se manejan los túneles.
De aquí queda claro que el uso de las dos pilas IPv4 e IPv6 así como el uso de túneles serán usados hasta que se llegue a tener una red IPv6 nativa.
Tal vez habrá algunos equipos como los de seguridad (firewall) principalmente a los que habrá que actualizar o modificar algo en su configuración, ya que no permiten pasar ni un simple ping aun cuando este vaya encapsulado con direcciones IPv4, lo que se debe a que estos equipos hacen una inspección a fondo del paquete que esta intentando pasar y cuando se dan cuenta que el paquete que encapsula a IPv6 especifica en su campo de protocolo el numero 41 correspondiente a IPv6 lo descartan, por ser este numero de protocolo nuevo y

como los equipos de seguridad no lo conocen ni entienden no lo dejan pasar puesto que para ellos se puede estar tratando de un engaño (spoofing), lo cual es un truco muy común por parte de los hackers para burlar la seguridad de los equipos, ya que muchas veces hacen spoofing indicando cierto protocolo cuando en realidad están disfrazándose para pasar y encontrar huecos o vulnerabilidades en un sistema.

Por las pruebas que se realizaron sea cual sea el prefijo de dirección que se utilice (link local-FE80, site local FEC0, temporales 3FFE, isatap fe80::5efe:w.x.y.z, v4compatibles ::w.x.y.z o globales 2002) la resolución de nombres en cada una de ellas funciona, la seguridad con cada una de ellas funciona, así como el ping, tracert, pathping, telnet, ftp y http.

El protocolo http solamente se checo en las ultimas pruebas realizadas con direcciones globales 6to4 (23002) pero por los resultados obtenidos con las pruebas realizadas con los otros protocolos este también debe funcionar perfectamente con los primeros tipos de direcciones probados.

5. COMPARATIVO DE LA MIGRACIÓN

Cuando se realiza el cambio de un sistema, normalmente se debe a que el nuevo sistema representa una nueva tecnología que presenta grandes características respecto al otro que lo hacen sumamente diferentes y atractivo, lo que alienta de sobremanera su adopción, adicionalmente el nuevo sistema viene a cubrir algunas deficiencias del sistema anterior.
Podríamos decir que el funcionamiento actual de las redes locales así como de Internet con el protocolo IPv4 resulta ser muy satisfactorio, de hecho si no fuera por el problema del agotamiento de las direcciones IP de 32 bits (que entre otros problemas este es el de mayor peso), aunque con algunas otras deficiencias el protocolo IPv4 no tendría muchas razones de peso para ser cambiado y podría continuar siendo uno de los protocolos mas usados.

5.1 COMPARACION DE VELOCIDADES CON IPV4 Y CON IPV6

Si se realiza la comparación de IPv4 con IPv6 en lo que a velocidades se refiere teóricamente deben ser percibidos algunos cambios como el aumento de velocidad en IPv6 con respecto a IPv4, asimismo debe notarse un mejor desempeño en una red con IPv6 respecto a IPv4.
En una red debe notarse la mejora en desempeño de la red local. Con IPv4 cuando un host se quiere comunicar con otro realiza un broadcast para conocer la dirección física o MAC del nodo destino, ya que la dirección fuente para poder mandar información a su destino usa la dirección del nivel de enlace o dirección de control de acceso al medio, si este nodo fuente no conoce dicha dirección física ejecutara un broadcast por medio del uso del protocolo ARP a todos los nodos que están conectados a la red LAN, este broadcast llega a todos los nodos, tanto al interesado como a los no interesados, este proceso de broadcast además de inundar la red en ese instante provoca en todos los hosts al recibir ese paquete una pequeña interrupción en su funcionamiento para poder atender la petición y comprobar si ellos son el nodo solicitado, esta interrupción es provocada tanto en los nodos IP como en los que no manejan IP.
En IPv6 los procesos de broadcast son eliminados, ahora la comunicación es mediante transmisión unicast o multicast, esto debe hacer que el desempeño de la red local sea mejor. con las pruebas realizadas pudimos comprobar que la búsqueda de un nodo destino se hace efectivamente por multicast, lo cual puede parecer todavía como que se mandan muchos paquetes multicast a todos los nodos de cierto grupo cuando solo queremos conocer a uno, durante las pruebas realizadas pudimos observar que este proceso de multicast es un multicast prácticamente dirigido al nodo destino, si se usan las direcciones formadas con su parte de identificador de host en formato EUI-64, cuando un nodo hace una petición de conexión a otro nodo ya sea que se le especifique la dirección IPv6 destino tal cual es (en formato de 8 campos de 4 caracteres hexadecimales cada uno separados por :), o el nodo solicite la dirección IPv6 del nodo destino a un servidor DNS, le será regresada esta dirección con los últimos 64 bits del identificador de hosts en formato EUI-64 también, como sabemos la construcción de la parte del identificador de hosts en una dirección IPv6 se basa en la dirección MAC, por lo que el nodo fuente sabe que la dirección física esta

contenida en los últimos 64 bits de la dirección IPv6 destino que esta buscando, entonces el nodo fuente tomara los últimos 4 bytes de esa dirección IPv6 para realizar el multicast, entonces la búsqueda de la dirección física por multicast dirigido de un nodo es casi directa al nodo destino, esto lo podemos ver en el siguiente paquete capturado durante las pruebas con direcciones link local, donde antes de realizar un ping, un nodo fuente busca a un nodo destino por multicast:

C:\Documents and Settings\cliente1>ping **fe80::20d:9dff:fe55:2f41**%13
Haciendo ping a fe80::20d:9dff:fe55:2f41%13 con 32 bytes de datos:

Respuesta desde fe80::20d:9dff:fe55:2f41%13: tiempo<1m
Respuesta desde fe80::20d:9dff:fe55:2f41%13: tiempo<1m
Respuesta desde fe80::20d:9dff:fe55:2f41%13: tiempo<1m
Respuesta desde fe80::20d:9dff:fe55:2f41%13: tiempo<1m

Estadísticas de ping para fe80::20d:9dff:fe55:2f41%13:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 0ms, Máximo = 0ms, Media = 0ms

Se esta realizando un ping al nodo con dirección **fe80::20d:9dff:fe55:2f41**, para esto el nodo fuente primero hace una búsqueda de vecino (neighbor solicitation) para conocer su dirección MAC, antes de hacer la petición de ping:

```
No.     Time        Source                Destination           Protocol
Info
      1 0.000000    fe80::20b:cdff:fea9:528b ff02::1:ff55:2f41     ICMPv6
Neighbor solicitation

Frame 1 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Dec 21, 2004 17:36:53.499250000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0b:cd:a9:52:8b, Dst: 33:33:ff:55:2f:41
    Destination: 33:33:ff:55:2f:41 (IPv6-Neighbor-Discovery_ff:55:2f:41)
    Source: 00:0b:cd:a9:52:8b (CompaqHp_a9:52:8b)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::20b:cdff:fea9:528b   NODO FUENTE
    Destination address: ff02::1:ff55:2f41     MULTICAST A LOS ULTIMOS 4
                                               BYTES DEL DESTINO
```

```
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0x3de3 (correct)
    Target: fe80::20d:9dff:fe55:2f41
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0b:cd:a9:52:8b

0000  33 33 ff 55 2f 41 00 0b cd a9 52 8b 86 dd 60 00   33.U/A....R...`.
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 02 0b   ... :...........
0020  cd ff fe a9 52 8b ff 02 00 00 00 00 00 00 00 00   ....R...........
0030  00 01 ff 55 2f 41 87 00 3d e3 00 00 00 00 fe 80   ...U/A..=.......
0040  00 00 00 00 00 00 02 0d 9d ff fe 55 2f 41 01 01   ...........U/A..
0050  00 0b cd a9 52 8b                                 ....R.

No.     Time        Source                Destination           Protocol
Info
    2  0.000000       fe80::20d:9dff:fe55:2f41  fe80::20b:cdff:fea9:528b
ICMPv6   Neighbor advertisement

Frame 2 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Dec 21, 2004 17:36:53.499250000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 2
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 00:0b:cd:a9:52:8b
    Destination: 00:0b:cd:a9:52:8b (CompaqHp_a9:52:8b)
    Source: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::20d:9dff:fe55:2f41
    Destination address: fe80::20b:cdff:fea9:528b
Internet Control Message Protocol v6
    Type: 136 (Neighbor advertisement)
    Code: 0
    Checksum: 0x90f5 (correct)
    Flags: 0x60000000
        0... .... .... .... .... .... .... .... = Not router
        .1.. .... .... .... .... .... .... .... = Solicited
        ..1. .... .... .... .... .... .... .... = Override
    Target: fe80::20d:9dff:fe55:2f41
    ICMPv6 options
        Type: 2 (Target link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41

0000  00 0b cd a9 52 8b 00 0d 9d 55 2f 41 86 dd 60 00   ....R....U/A..`.
```

8 campos componen al datagrama de IPv6

```
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 02 0d   ... :...........
0020  9d ff fe 55 2f 41 fe 80 00 00 00 00 00 00 02 0b   ...U/A..........
0030  cd ff fe a9 52 8b 88 00 90 f5 60 00 00 00 fe 80   ....R.....`.....
0040  00 00 00 00 00 00 02 0d 9d ff fe 55 2f 41 02 01   ...........U/A..
0050  00 0d 9d 55 2f 41                                 ...U/A

No.     Time        Source                Destination           Protocol
Info
      3 0.015625       fe80::20b:cdff:fea9:528b  fe80::20d:9dff:fe55:2f41
ICMPv6   Echo request

Frame 3 (94 bytes on wire, 94 bytes captured)
    Arrival Time: Dec 21, 2004 17:36:53.514875000
    Time delta from previous packet: 0.015625000 seconds
    Time since reference or first frame: 0.015625000 seconds
    Frame Number: 3
    Packet Length: 94 bytes
    Capture Length: 94 bytes
Ethernet II, Src: 00:0b:cd:a9:52:8b, Dst: 00:0d:9d:55:2f:41
    Destination: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)
    Source: 00:0b:cd:a9:52:8b (CompaqHp_a9:52:8b)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source address: fe80::20b:cdff:fea9:528b
    Destination address: fe80::20d:9dff:fe55:2f41
Internet Control Message Protocol v6
    Type: 128 (Echo request)
    Code: 0
    Checksum: 0xe864 (correct)
    ID: 0x0000
    Sequence: 0x00af
    Data (32 bytes)

0000  00 0d 9d 55 2f 41 00 0b cd a9 52 8b 86 dd 60 00   ...U/A....R...`.
0010  00 00 00 28 3a 80 fe 80 00 00 00 00 00 00 02 0b   ...(:...........
0020  cd ff fe a9 52 8b fe 80 00 00 00 00 00 00 02 0d   ....R...........
0030  9d ff fe 55 2f 41 80 00 e8 64 00 00 00 af 61 62   ...U/A...d....ab
0040  63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72   cdefghijklmnopqr
0050  73 74 75 76 77 61 62 63 64 65 66 67 68 69         stuvwabcdefghi
```

Lo subrayado y en negrita, nos indica que el nodo fuente hace un multicast ff hacia los nodos en el mismo enlace 02 pero dirigido al nodo o servidor con los últimos 4 bytes igual a ff55:2f41, es decir esta solicitud de vecino (**ff02::1:ff55:2f41)** llegara a los nodos que tengan como parte de su dirección MAC ff55:2f41, esto resulta en una mejora del desempeño de la red ya que estos tipos de transmisiones no interrumpen la labor de los todos los nodos, al mismo tiempo hay menos paquetes circulando por la red comparados con los que existen con el uso de broadcast.

Si a lo anterior le agregamos que una estación a nivel de enlace puede determinar que paquetes multicast recibir, mientras que los paquetes de broadcast esta obligada a recibirlos.

Con esta característica de multicast dirigido una red LAN deberá funcionar mejor.
En el caso de la red LAN usada no se logro constatar esta mejora ya que el laboratorio de pruebas tuvo que convivir con la red entera que era IPv4 y aunque si pudimos verificar el uso de multicast dirigidos no se pudo apreciar un cambio significativo en el desempeño de la red y velocidad de la red.
Por otro lado cuando se interconectan varios subredes mediante ruteadores debe notarse un mejora en cuanto a la velocidad de transmisión y desempeño de los equipos ruteadores, ya que como sabemos los paquetes de IPv6 están optimizados para que los ruteadores no inviertan demasiado tiempo en su procesamiento, esto por una parte debido a que los datagramas IPv6 tienen menos campos que los de IPv4, por lo que si un router antes revisaba 12 campos y por así decirlo tardaba 12 microsegundos en revisar los 12 campos ahora solo tardara 8 por que los datagramas de IPv6 solamente tienen 8 campos, esto se puede verificar en el anterior paquete capturado, donde cada paquete de neighbor solicitation, advertisement, echo request tienen un encabezado IPv6 con 8 campos.
Con IPv4, algunos campos requerían que los ruteadores ejecutaran ciertas funciones que le restaban velocidad a cada equipo por donde pasaba el paquete para ejecutar la misma función, ahora serán realizadas solamente por los extremos, como es el caso de la fragmentación que será realizada por los nodos en comunicación, por lo que al quitarle el trabajo al router de realizar la fragmentación se le quita ciertas actividad que le restaba tiempo y velocidad de expedición o retransmisión del paquete.
En el laboratorio implementado se crearon 3 subredes diferentes y se conectaron por medio de ruteadores IPv6, también se hizo pasar el trafico IPv6 encapsulado por un router motorola IPv4 nativo insertado en medio de las subredes, las pruebas realizadas con ping, tracertr, pathping, telnet, ftp y http funcionaban en forma correcta pero no se apreciaron las bondades de los nuevos campos optimizados de IPv6 en una mejoría en cuanto a velocidad debido a que no se hizo una transportación de gran cantidad de información, con el uso de ftp podríamos haber visto un mejor comportamiento de IPv6 con cierta cantidad de información al realizar la transmisión de archivos de información grandes, pero desgraciadamente en nuestro caso el servicio de ftp de Microsoft al parecer no tiene modificados los APIs para aceptar conexiones con direcciones IPv6 ya que aunque se observaba durante las pruebas que se realizaba un dialogo mediante ftp (de sincronía) entre los nodos, pero no se podía concretar la conexión.
Lo que sí pudimos por ejemplo constatar en una de las pruebas realizadas cuando se configuro la seguridad entre los nodos de extremo a extremo de nuestro laboratorio que cuando se realizaba la conexión por telnet era demasiado lenta e incluso después de logearnos en el servidor destino la conexión se quedaba pasmada y se desconectaba, lo cual podría atribuirse a IPv6 directamente o al uso del proceso de la autenticación, el primer aspecto se descartaba ya que durante las pruebas realizadas sin seguridad no se tenia este problema, solamente cuando se implementaba la seguridad, además este detalle se presento cuando se realizaba el encapsulamiento de IPv6 sobre IPv4, por lo que se modifico el tamaño del MTU de la pseudo interfaz que realiza el encapsulamiento, se aumento este parámetro y la conexión telnet se agilizo, Además después de logearse ya no se quedaba pasmado y los comandos tecleados en el nodo remoto respondían inmediatamente.
Cuando se conecto el laboratorio de pruebas a Internet por medio de túneles dinámicos 2002, se realizaron las mismas pruebas, se hicieron ping, tracert, pathping, telnet, ftp y http a sitios IPv6 las pruebas realizadas funcionaban perfectamente, incluso en este caso con algún sitio que tenia habilitada la conexión por ftp se realizo esta sin ningún problema.

En este punto hay que tomar en cuenta un detalle al realizar la comparación entre IPv6 e IPv4 cuando se realizan las pruebas hacia Internet, actualmente todas las conexiones hacia sitios IPv6 o al backbone de IPv6 de pruebas 6BONE se realizan por medio de túneles que dejan pasar el trafico de paquetes IPv6 dentro de paquetes IPv4, por lo que si se quiere verificar la mejoría en cuanto al desempeño de routers con IPv6 será difícil comprobarlo de esta forma. Ya que seguimos en realidad pasando por una infraestructura de IPv4 nativa, esto es, al encapsular un paquete de IPv6 en uno de IPv4, los routers de Internet analizaran los campos del paquete IPv4, los campos del paquete IPv6 serán revisados al salir del túnel IPv4, esto será durante el tiempo que dure la migración y se usen pilas dobles con ambos protocolos y túneles para comunicar a través de Internet un obstáculo para poder apreciar las bondades y mejoras en cuanto a velocidad o mejora de desempeño de los equipos con IPv6.

5.2 COMPARACION DE SERVICIOS OFRECIDOS CON IPv4 e IPv6

Como IPv6 es una versión nueva de IPv4, este puede ser aplicado con la misma infraestructura existente, el cambio más significativo es a nivel hardware. A nivel funcionamiento es prácticamente el mismo por lo que se pueden seguir usando tanto protocolos existentes y aplicaciones actualizadas para que tengan la capacidad de manejar las nuevas características de IPv6.

La comparación de IPv4 e IPv6 deberá ser realizada en base a la apreciación de las nuevas características que ofrece.

Se tiene que tomar en cuenta al momento de comparar IPv4 con IPv6, que IPv6 no surgió por que IPv4 sea ya un sistema obsoleto. Por lo que tal vez se esperen fuertes cambios en cuanto al funcionamiento y tecnología, cambios que no serán visibles en una primera instancia como sucede a menudo con los cambios de tecnología. Es decir IPv6 es muy parecido a IPv4, incluye las características de IPv4 y agrega otras adicionales, lo que implica que tal vez no se requiera realizar una migración total tanto en hardware como en software.

El caso de IPv6 podría ser comparado al caso de cuando se libera una nueva versión de sistema operativo de Windows, es el mismo sistema operativo con otra apariencia y ciertas mejoras pero en esencia y funcionamiento es el mismo.

Con IPv6 sucede algo parecido, de hecho IPv6 se define como la nueva versión del protocolo de Internet IP mas no decimos que es un nuevo protocolo de Internet, por ello el gran numero de aplicaciones de IPv4 que funcionan actualmente deberán funcionar con IPv6 con sus respectivas modificaciones de las APIs.

Los mismos servicios y aplicaciones que ofrece IPv4, son ofrecidos con IPv6, así, tenemos aplicaciones ya en uso y probadas para IPv6 como Telnet, http, FTP, correos, DNS.

Un gran numero de fabricantes de aplicaciones así como de software han realizado los cambios necesarios a sus aplicaciones y los servicios que estas ofrecen para poder manejar el protocolo IPv6.

La comparación entre las aplicaciones de IPv6 e IPv4 tal vez no pueda ser un punto clave de comparación entre ambas versiones de IP, ya que IPv6 no se diseño por que IPv4 no pudiera con las aplicaciones que corren sobre el, IPv6 se diseño para arreglar ciertas

dificultades que se vislumbraron serian un problema para IPv4 en un futuro cada vez más cercano.
IPv6 además de funcionar transparentemente con las aplicaciones ya existentes, permitirá desarrollar nuevas aplicaciones así como hará realidad otras que estaban frenadas.
Entre otras cosas IPv6 permitirá aplicar la calidad de servicio al trafico que utilice IPv6, algo muy importante para permitir el despegue de aplicaciones como videoconferencias, multimedia, en el proceso de convergencia de aplicaciones sobre Internet, la convergencia es un tema que se viene cocinando desde hace tiempo y que muchas empresas ven como las redes del futuro pero no podía llevarse a cabo entre otras cosas por la falta del aseguramiento de la calidad para el manejo de trafico mas delicado que los datos como son el video, la voz, etc. esto debido a la naturaleza de IP, ya que al ser un protocolo que hace su mejor esfuerzo para hacer llegar los paquetes a su destino no asegura que ciertos flujos de información que requieran mayor velocidad o mas ancho de banda lo tengan, IPv4 veía todo el trafico voz, datos, video, imágenes multimedia como igual, el no distinguía si era uno u otro por lo que se le daba el mismo trato. Con las facilidades de los campos correspondientes de IPv6 de prioridad y etiqueta de flujo la selección de aplicación de ciertos criterios para el trafico más delicado podrá ser implementada en este nivel.
Asimismo la capacidad del aseguramiento del trafico circulando por Internet era un tema de mucho interés para las empresas ya que con el uso de Internet para el transporte de todo tipo de trafico para conectar empleados a la empresa, sucursales o intranets de otras empresas por Internet pasando probablemente información confidencial por este medio hacia necesario contar con seguridad necesaria para confiar en este tipo de comunicación, con IPv4 dicha seguridad era implementada a otros niveles diferentes del de Internet como por ejemplo a aplicación mediante firewall, proxies u otras aplicaciones exclusivas para ello, lo que implicaba la adquisición de hardware, software, capacitación y complejidad adicional a la red. Con IPv6 esta seguridad es una obligación implementada intrínsecamente en el mismo protocolo a nivel de red. Cualquier aplicación que corra sobre IP será protegida, incluso aun saliendo desde el mismo nodo origen lo que asegura la información de extremo a extremo.
Durante pruebas se habilito la seguridad en diferentes esquemas de conexión y con los diferentes tipos de direcciones IPv6, para lo cual aplicamos la seguridad IPsec usando los protocolos AH (Authentication Header) y ESP (Encapsulation Security Payload), dicha seguridad fue aplicada desde los hosts mismos con Windows XP y en los routers también, este sistema operativo permite aplicar estos protocolos de seguridad con autenticación HMAC-MD5, los cuales pueden usarse en modo transporte o en modo túnel. Para las pruebas se uso la seguridad IPSEC tanto con AH como ESP con direcciones link local, con direcciones site local, y con direcciones globales 6to4 en esta ultima se combinaron los protocolos para encapsular el trafico con ESP haciéndolo pasar por un túnel AH entre los gateways de seguridad que en este caso eran los routers que conectaban las subredes donde se encontraban ambos nodos, para todas las pruebas se uso una llave simétrica precompartida en modo texto. Las pruebas implementadas mediante la seguridad funcionaron sin ningún problema y correctamente para todas las pruebas realizadas con ping, tracert, pathping, telnet, ftp, http.
IPv6 presenta una característica que como aplicación va a dar mucho de que hablar en el futuro, se trata de la movilidad, la movilidad representara un gran apoyo para las nuevas aplicaciones que se están gestando en los grandes proveedores de telefonía de tercera generación para el ofrecimiento de servicios de Internet a sus usuarios, esta movilidad se

vislumbra como una aplicación a gran escala para proveedores de Internet para usuarios que viajan continuamente y desean acceder a Internet desde cualquier punto así como a las instalaciones corporativas de su empresa, hogar, etc.
Se pudo constatar que por las características de IPv6 se tienen muchas facilidades para que se pueda llevar a cabo la aplicación de movilidad, gracias a las características que tiene IPv6 de plug and play. En las pruebas realizadas pudimos constatar que inmediatamente después de conectarse a la red local con la pila IPv6 activada cualquier nodo automáticamente autoconfigura una dirección IPv6 aun sin recibir algún anunciamiento de router o una dirección asignada por un servidor DHCP6, y sin tener ninguna configuración manual, con dichas direcciones el nodo se puede comunicar inmediatamente con los demás hosts, de la red local. Además de la dirección local que por default cualquier nodo autoconfigura, si recibe un anunciamiento de router en el cual se indica el prefijo usado por la red cualquier nodo también autoconfigura las direcciones IPv6 con el prefijo recibido sin intervención de ningún tipo, según sea el prefijo anunciado se autoconfiguran direcciones del tipo site local, temporales 3ffe o globales 2002, este tipo de configuración de direcciones también puede ser realizado mediante diálogos con servidores DHCP para que con ciertas funciones de control se asignen direcciones al nodo, características como estas permitirán la implementación mas sencilla de aplicaciones para dispositivos o usuarios móviles que requieran tener conectividad a las redes que se conecten en cualquier lugar.
Otro punto fuerte que se vislumbra para ser cubierto por IPv6 gracias a su gran capacidad de direccionamiento que permitirá tener conectividad por medio de Internet a millones de dispositivos como televisores por cable, acceso de banda ancha a los hogares permanente conectados, celulares, PDAs, aparatos electrodomésticos, laptops, sistemas de monitores, refrigeradores, lavadoras y un gran numero de aplicaciones que se han estado planeando desde hace algún tiempo para ofrecer los servicios de Internet pero que por las mismas dificultades de conectividad debidas al escaso numero de direcciones IPv4 era difícil otorgar, con IPv6 esto ahora no es ningún problema y se vislumbra que sea realidad en un futuro cercano.

5.3 COMPARACION DE MANEJO DE LA SEGURIDAD

En IPv6 el manejo de seguridad no es un servicio opcional, es una obligación requerida desde que se planteo y definió el nuevo protocolo, en IPv4 este servicio es opcional, normalmente es implementado a nivel aplicación vía aplicaciones o firewalls.
En la red LAN propuesta para la migración no se tenia implementado un sistema de seguridad a nivel IPv4, se llegaba a utilizar la seguridad IPsec a partir del firewall cuando se establecían VPNs hacia el Internet, Fig. 5.3.1,

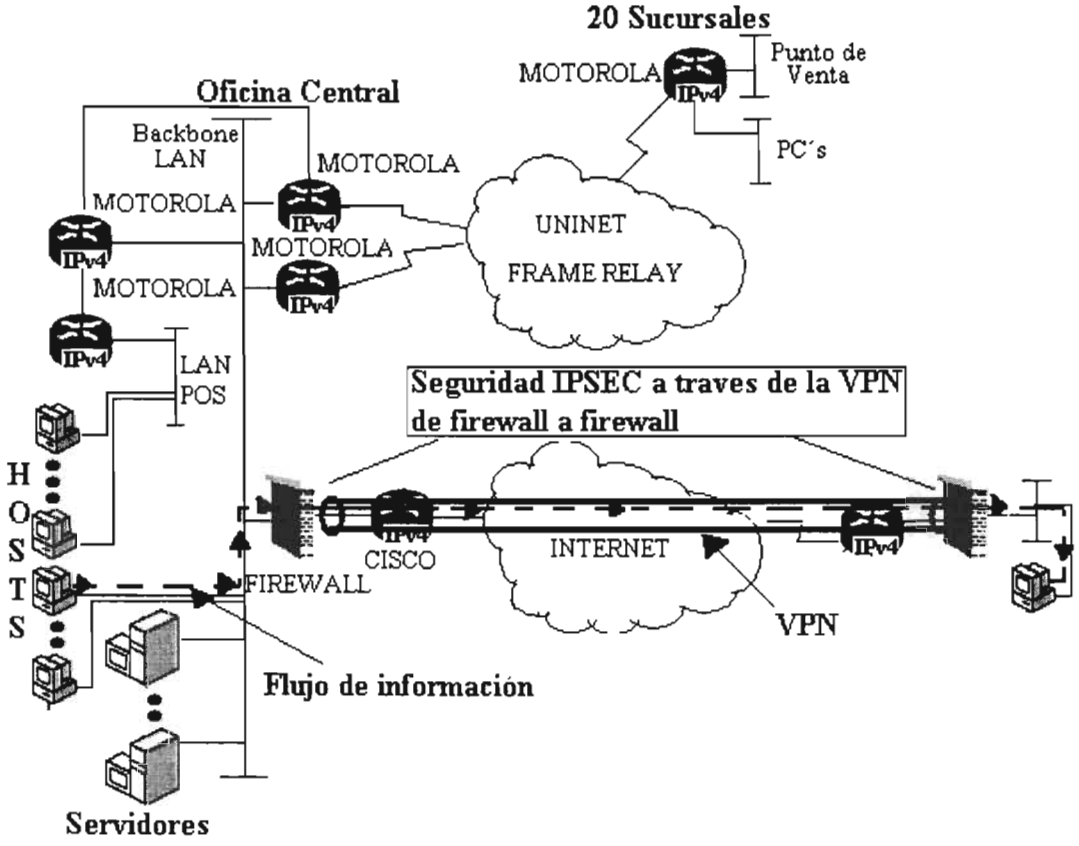


Fig. 5.3.1 Seguridad en IPv4 a través de los firewall

Este tipo de seguridad no era una seguridad de extremo a extremo, puesto que la seguridad solamente protegía la información en las fronteras de las redes conectadas:
En IPv6 al ser obligatorio el manejo de la seguridad, esta puede ser configurada desde los extremos mismos, Fig. 5.3.2.

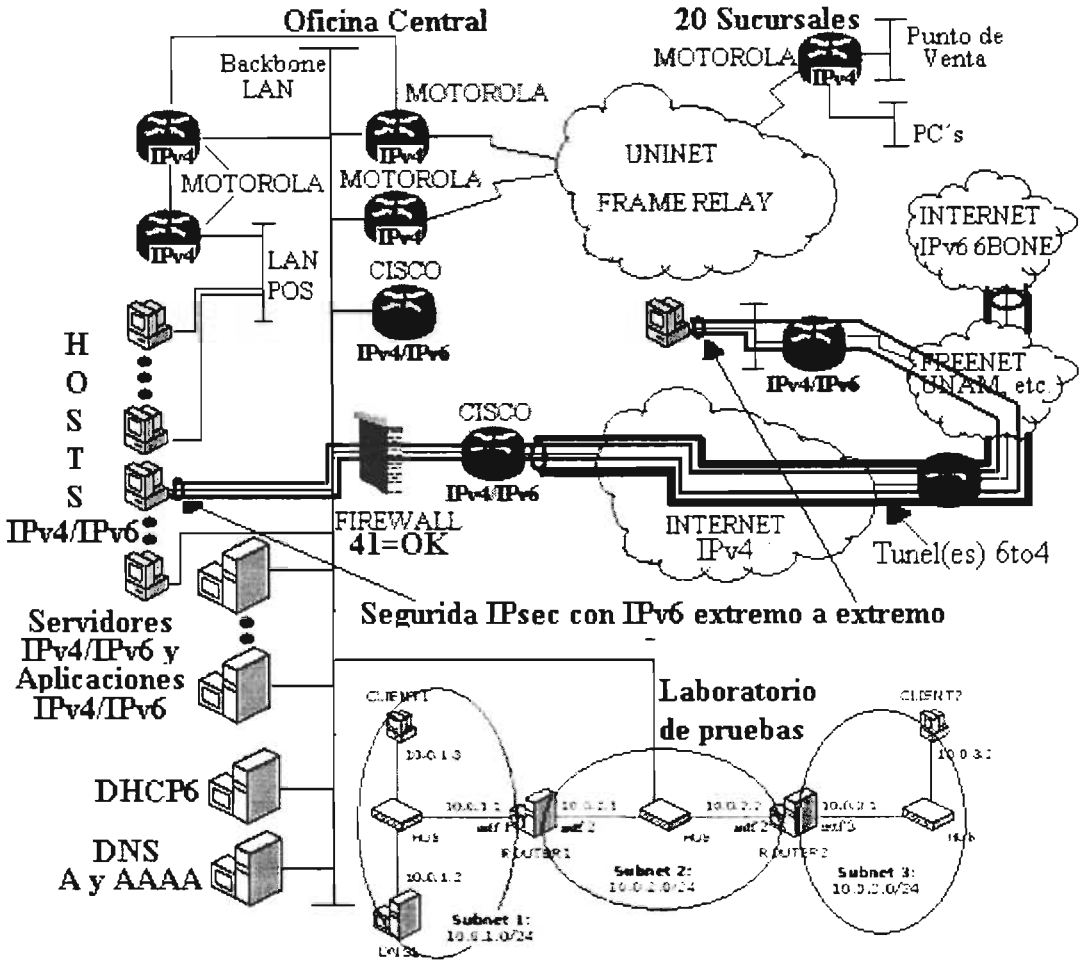


Fig. 5.3.2 Seguridad IPsec con IPv6 de extremo a extremo a nivel de red

En el laboratorio conectado al backbone de la red LAN se implemento la seguridad IPsec con diferentes esquemas, para lo cual se usaron los protocolos AH y ESP en modo transporte y modo túnel.

Las pruebas realizadas con seguridad IPsec funcionaron correctamente, se capturo el trafico en los nodos en los que se implemento la seguridad y se observaron los procesos de encapsulamiento y desencapsulamiento con AH y ESP.

Como podemos ver en la red LAN se usaba seguridad IPsec en IPv4 solamente cuando se establecían VPNs a Internet, seguridad que solamente protegía al trafico dirigido al sitio conectado por la VPN. Con IPv6 podemos asegurar el trafico de extremo a extremo y todo el trafico que circule hacia Internet, ya que se puede aplicar este tipo de seguridad desde el nodo mismo que genera la información, así como en los routers por los que pasa este trafico.

6. EVALUACION Y UNA RECOMENDACIÓN TECNICA Y ECONOMICA

Aunque IPv4 es la forma más usual de comunicación entre redes TCP/IP, IPv6 se esta introduciendo poco a poco en las aplicaciones y sistemas operativos.
El cambio a IPv6 tiene muchas ventajas y resuelve problemas o deficiencias actuales de IPv4 pero representara para las organizaciones publicas y privadas inversiones en la actualización de software, hardware, capacitación del personal administrativo de sistemas, uso y replanteo de nuevos estándares y definitivamente tiempo para llevar a cabo dicho cambio. A cambio de esto se estiman beneficios en términos de autoconfiguración, seguridad y movilidad entre muchos otros, dichos beneficios podrían inclinar la balanza costo-beneficio a favor del cambio a IPv6.
Muchas aplicaciones han liberado versiones funcionales con el estándar IPv6 y muchas redes en el mundo ya funcionan con IPv6.
Las diversas ventajas de IPv6 y el análisis costo-beneficio forman un argumento a favor de la migración para los administradores de sistemas. Dichas ventajas son por ejemplo, la comunicación que deberá seguir existiendo entre las redes IPv4 e IPv6, la transición puede realizarse en forma gradual, IPv6 puede descubrir automáticamente la información que necesita para conectarse a Internet sin intervención de un administrador, o bien también puede hacerse a través de un sistema con DHCP, también el protocolo tiene características que ayudaran a manejar prioridades en la transmisión de información y optimizar los recursos de red, la característica de seguridad intrínseca con IPsec resulta también un elemento atractivo del protocolo ya que evita la necesidad de nuevas capas de seguridad.
La evaluación técnica y económica se realizo tratando de mantener la visión de que la actualización a IPv6 se realizara en la forma mas transparente a la red, así como la inversión económica lo menor posible.
Algunas personas manejan el proceso de cambio IPv4 a IPv6 como algo costoso y de enorme trabajo, pero tal vez con una planeación basada en la realización de los cambios necesarios por etapas, la transición no debería impactar el funcionamiento de la red, lo que a su vez ayudaría a que los costos no resultaran tan elevados.
Desde mi punto de vista creo que se puede ver este proceso como si fuera el upgrade de las PCs, servidores, aplicaciones o ruteadores a una versión nueva de IP, como cuando se actualiza un ruteador a una nueva versión de sistema operativo la cual tiene características nuevas y más avanzadas, si quitamos las nuevas características seguimos teniendo el mismo sistema operativo. Así por ejemplo se tienen que actualizar las PCs y servidores para que manejen las dos pilas de IP en una primera etapa lo cual se puede hacer aplicando un parche si existe o actualizando el sistema operativo a Windows XP, es decir estamos aplicando el mismo procedimiento que aplicamos cuando actualizáramos el sistema operativo de Windows 95 a 98.
Las aplicaciones se actualizan para que manejen también las dos versiones de IP, dichas aplicaciones son desarrolladas por los fabricantes de software quienes ya están encargándose de ello e incluso muchos ya las han liberado por lo tanto únicamente se tiene que aplicar la actualización correspondiente ya sea por nueva versión o parche, por ejemplo los grandes vendedores de sistemas operativos como Windows, unix, linux, bsd, están liberando parches para cargar el protocolo IPv6 a las versiones de sistema operativo

existentes, además están liberando sus nuevas versiones de sistemas operativos con la pila IPv6 integrada, gran parte de dichas actualizaciones se están liberando en forma gratuita. Los ruteadores también se deben actualizar para manejar ambas pilas de protocolos tal y como normalmente hacemos para actualizar el sistema operativo del ruteador para manejar algún protocolo nuevo o característica más avanzada de un nuevo release, si se tiene un contrato con el proveedor o fabricante de dichos equipos la descarga de dicho release es en forma normal sin costo adicional. En estas condiciones se encuentran un gran numero de empresas, lo que ofrece ciertas facilidades a la realización paulatina sin afectar tanto su funcionamiento y su economía.
Con este punto de vista se propuso la serie de pasos generales para la migración y para tratar que la inversión económica implicada en el proceso de migración no resulte tan costosa.

6.1 COEXISTENCIA DE IPV6 CON IPV4

Definitivamente se debe buscar y hacer cumplir la coexistencia de IPv4 con IPv6. Se debe perseguir el objetivo de esta coexistencia ya que es la principal condición para que la migración sea mas ampliamente aceptada. Se debe hacer que se cumpla dicha coexistencia para que la enorme infraestructura de IPv4 pueda de cualquier modo continuar comunicada con sistemas actualizados, ya que de otra manera se formarían islas aisladas de IPv6 en medio de la enorme red que representa la enorme infraestructura implementada actualmente con IPv4. o por el contrario si la mayor parte de la infraestructura IPv4 fuera actualizada habría ciertas zonas con IPv4 que quedarían incomunicadas, por lo que un punto fuerte que puede apoyar la coexistencia entre ambos protocolos es el uso de la estrategia de doble pila. por lo que si se formara una área mayor de IPv6 esta debería ser capaz de hablar con el área IPv4 mediante el manejo y soporte de los dos protocolos. La técnica del uso de túneles es otro punto apoya la convivencia de IPv4 con IPv6, ya que con esta técnica se puede hacer pasar el trafico IPv6 sobre la infraestructura IPv4 en forma transparente..
No seria posible siquiera pensar en realizar el cambio a IPv6 si no se cumple esta condición (coexistencia de IPv6 con IPv4), ya que por ejemplo, aun con la compatibilidad probada entre ambas versiones gracias a los diferentes mecanismos como el manejo de dobles pilas de protocolos, encapsulamiento de IPv6 en IPv4. direcciones IPv6 compatibles con IPv4. etc.. la gran mayoría de las empresas usuarias de IPv4, a la fecha, después de cumplirse casi 12 años de la definición de IPv6 ni siquiera se han interesado en dicho protocolo. Gran parte de esa falta de interés se debe a que con todo y sus limitaciones la gran infraestructura de IPv4 funciona de manera satisfactoria y seguirá haciéndolo mientras no se lleguen a enfrentar problemas como los de algunos países que apenas si tienen disponible una sola dirección clase C.
Debido a que IPv4 es un protocolo que ha provocado el desarrollo de mucha tecnología, de muchas aplicaciones, ha logrado comunicar al mundo entero. aun para mucha gente no se contempla o vislumbra el fin de este o que haya llegado a un tope, por que en realidad tiene para seguir dando buenos resultados por tiempo indeterminado. actualmente como trabaja IP lo hace muy bien y funciona perfectamente para lo que fue creado, pero también su popularidad ha provocado el desarrollo de muchas aplicaciones y servicios basadas en IP, debido a que en sus inicios no se vislumbro tanta popularidad. lo que además de las malas administraciones y asignaciones de sus direcciones así como defectos en su diseño original

(como el numero de bits para el direccionamiento, muchos campos a procesar por los equipos con lo que caen en redundancias al realizar tareas que protocolos de otras capas ya realizan), el protocolo requiere ser mejorado para poder seguir funcionando y seguir siendo el protocolo mas popularmente usado en todo el mundo.
Por lo anterior y por la enorme base de IPv4 instalada, IPv6 deberá seguir existiendo en una primera etapa junto con IPv4, ambos en cada nodo existente, para que ningún nodo pierda la comunicación con los demás nodos, servidores o aplicaciones existentes y que al mismo tiempo puedan hablar con los nodos, servidores y aplicaciones IPv6.
La convivencia de ambos protocolos deberá darse en cualquier parte de las redes internamente a una red local, en el limite de dicha red, en el acceso a Internet, en la plataforma de ruteo de los ISPs, etc.
Esta convivencia se ha probado que se puede dar tanto en nodos, servidores, aplicaciones, y ruteadores puede implementarse en hosts con la instalación de las dos pilas de protocolos IPv4 e IPv6, así como en los servidores, en las aplicaciones con sus APIs modificadas para que entiendan ambas estructuras de direcciones, en ruteadores para que puedan comunicar redes aun sin migrar con las que ya lo han realizado mediante el uso también de la doble pila de protocolos y los túneles.
Para que esta convivencia de IPv4 con IPv6 se cumpla se pueden implementar diversas estrategias como son:
a) Sistemas con doble pila
Con el sistema de doble pila se ejecutan ambos protocolos IPv4 e IPv6.
Características:

- El sistema se debe conectar a ambas redes IPv4 e IPv6.
- Se requieren por lo tanto direcciones IPv4 e IPv6.
- Si se obtienen enlaces nativos de IPv6 se debe administrar dos redes paralelas.
- Incremento en la complejidad del desarrollo de aplicaciones.
- Se deberá instalar la doble pila en nodos, servidores, ruteadores.
- Tiene la ventaja que tanto los clientes IPv4 e IPv6 pueden acceder a los servicios y se evitan los problemas de los mecanismos de traducción.

b) Túneles
Con los túneles se conectan islas IPv6 a través de la infraestructura IPv4.
Características:

- Los túneles son transparentes a la aplicación.
- Es más complejo el enrutamiento.
- Actualmente se usan extensamente en redes IPv6 experimentales.
- Con una sola red podemos comunicarnos con nodos IPv4 y nodos IPv6.

c) Mecanismos de traducción
Los mecanismos de traducción permiten comunicación entre interlocutores IPv6 e IPv4.
Características:

- Pueden necesitar módulos específicos para algunas aplicaciones.
- Tienen Problemas de escalabilidad.
- Deben mantener información de los flujos IP.
- Es recomendable que se utilicen solo sí una aplicación: 1) No soporta la comunicación con ambos protocolos, 2)O se ejecuta en una maquina con una única pila. 3)O se tiene una maquina con doble pila pero la red solo soporta uno de los protocolos.

d) El mecanismo de aplicación más amplia es NAT-PT.

Las estrategias de pila doble y el uso de túneles son más viables como principio de migración hacia IPv6, la propuesta es que se instale el protocolo IPv6 junto al de IPv4 en los nodos, servidores y routers y que las aplicaciones se actualicen para que manejen ambas pilas.
Con las pruebas realizadas en el laboratorio pudimos comprobar que se puede realizar la migración a IPv6 y la comunicación entre los equipos que se vayan actualizando con los equipos que no se han actualizado o no se piensan actualizar sigue funcionando perfectamente a través del manejo de la doble pila y que junto con la utilización de los túneles IPv6 en IPv4 permitirá perfectamente hacer convivir las islas IPv6 con el resto de la red IPv4.
En uno de los esquemas del laboratorio que se probaron, se configuro una subred IPv6 con una Intranet IPv4 y se probo que se pudieran comunicar normalmente los nodos de la subred IPv6 con los nodos de la Intranet IPv4, gracias al manejo de las pilas y al encapsulamiento de trafico IPv6 en IPv4 mediante un router ISATAP, también se conecto una subred IPv6 a Internet mediante un router IPv4/IPv6 con una dirección publica homologada para crear un túnel dinámico hacia el router relay de Microsoft y se probo la comunicación desde nuestra subred IPv6 hacia sitios en el 6BONE mediante ping, tracert, pathping, telnet, ftp, http, estas mismas pruebas se realizaban hacia sitios IPv4 y la conectividad seguía funcionando normalmente por medio de la pila IPv4.
Con las pruebas realizadas y los resultados obtenidos y capturados mediante el sniffer Ethereal comprobamos que la convivencia de IPv4 e IPv6 funciona perfectamente.

6.2 COSTOS DE CAPACITACION

La parte de capacitación no debiera implicar una inversión significativa ya que IPv6 mantiene muchas características y gran parte del funcionamiento de IPv4 a las cuales agrega muchas mejoras y nuevas características por que el funcionamiento en forma general es igual pero con ciertas mejoras y sus propias formas de hacer las cosas por parte de IPv6. En un mundo de tecnología tan cambiante, hoy manejamos cierto sistema operativo y mañana ya surgió un nuevo reléase de dicho sistema operativo, el cual no resulta tan difícil de manejar si ya manejábamos el anterior, en un principio bastara con familiarizarse con las nuevas características de IPv6 y aplicarlas con lo que IPv6 podrá empezar a ser dominado.
El personal con conocimientos o manejo de IPv4 no tendrá que invertir demasiado en capacitación para conocer o manejar el nuevo protocolo, con los conocimientos de IPv4 solo se necesitan conocer algunos nuevos conceptos o características de el nuevo protocolo para poderlo manejar.
En caso de requerirse capacitar al personal para el manejo del protocolo IPv6 teniendo en cuenta que se deben tener los conocimientos del funcionamiento del protocolo de IPv4, a continuación tenemos costos de cursos de algunas instituciones sobre el manejo de IPv6:

Institución	Inversión
Informática Integrada Internetworking	$ 590.00 dls.
Tecnológico NYCE	$ 600.00 dls.

Si se requiere capacitación para el manejo de Windows XP y Windows server 2003, los costos serian:

Institución / curso	Costo
Windows XP	$ 610.00 dls
Windows server 2003	$ 610.00 dls
Windows 2000	$ 410.00 dls
Linux	$ 700.00 dls.

Se usa la cotización de Windows XP y Windows Server 2003 ya que Windows XP es el sistema operativo base de la red Lan propuesta y Windows Server 2003 puede tomar diferentes roles de servidor como DNS, DHCP, etc. por lo que puede ser usado para la instalación de los servidores DNS y DHCP6 para el manejo de direcciones IPv6 con nombres y la configuración stateful de direcciones.

6.3 COSTOS POR ACTUALIZACION DE HARDWARE

Los costos por hardware no deberían ser tan elevados ya que normalmente los equipos con que se cuenta actualmente si el fabricante libera versiones de sistema operativo para IPv6, dichos equipos son capaces de manejar IPv6, a menos que el fabricante especifique que la versión requiera cambio de equipos, como el cambio a IPv6 puede ser visto como una actualización de versión de IP, no debería implicar un cambio completo de la infraestructura tecnológica. A menos que el hardware actual no sea capaz de manejar tal cambio, el cambio de hardware se tendrá que realizar lo cual de cualquier modo puede ser realizado conforme a los planes de mantenimiento o actualización planeados.

De este modo en un router, PC o servidor si existe alguna versión para IPv6 se actualizara su sistema operativo, se aplicara un parche o se agregara solamente la pila de capa de red IPv6 a la actual IPv4, realmente esto no debiera requerir que se tenga que crecer una maquina en cuanto a su capacidad.

Probablemente habrá equipos como las PC's principalmente que por el sistema operativo que manejan, debido a que no existiera alguna versión o parche para su sistema operativo por parte del fabricante, se tendria que instalar un nuevo sistema operativo con soporte para IPv6 no solamente la pila del protocolo, normalmente un nuevo sistema operativo por ser más robusto requerirá mas recursos o cambio definitivo de equipo, aunque la gran mayoria de fabricantes de software, ya sea de plataformas o aplicaciones se están preocupando por incluir en sus nuevas versiones el soporte para IPv6, asi como por la liberación de parches o actualizaciones para sus versiones ya existentes, con dichos parches normalmente solo se adecua el software para el manejo de IPv6, parches que pueden ser soportados por el hardware existente.

En la red LAN propuesta tenemos tres áreas para analizar el costo de hardware:

- Las PCs. En el caso de los hosts o PCS no se necesita realizar la actualización de la pila, ya que todas las PCs son de reciente adquisición con el sistema operativo Windows XP preinstalado, el cual fue probado en el laboratorio de pruebas y funciona sin ningún problema.

- Los servidores. En cuanto a los servidores estimo que no se necesita realizar una actualización de hardware, ya que con las características que se tienen y si existen los parches necesarios, estos equipos pueden soportar la actualización de IPv6.
- Los switches. En la red propuesta aun se utilizan hubs para interconectar los equipos por lo que estos equipos tendrían que ser renovados por switches aprovechando el proceso de actualización y para apoyar el aprovechamiento de las características de IPv6.
- Los routers. En una primera opción y para no impactar el funcionamiento de la red, se pensó dejar la infraestructura de routers actual igual para lo que se propuso agregar un router para manejar el ruteo de IPv6 dentro de la red, hacia el Internet el equipo Cisco que se tiene puede seguir funcionando pero con el IOS actualizado. Sin embargo y como la base de ruteo instalada es Motorola que no soporta IPv6 se puede también proponer cambiar esta plataforma de ruteo por la marca Cisco.

En base a lo anterior, a continuación tenemos costos aproximados que se generarían en los cambios tanto de PCs, routers, firewall y switches para el manejo IPv6.

Si en la etapa inicial de conexión al 6BONE no se quisiera actualizar el router y en lugar de ello se quisiera poner una PC con dos tarjetas de red y una dirección publica homologada con la doble pila IPv4/IPv6 la cual funcionaria como nuestro router de salida a la red IPv6. De hecho durante las pruebas de laboratorio se uso este esquema de una PC router para conectarnos a Internet, la propuesta con esta PC router se muestra en la Fig. 6.3.1.

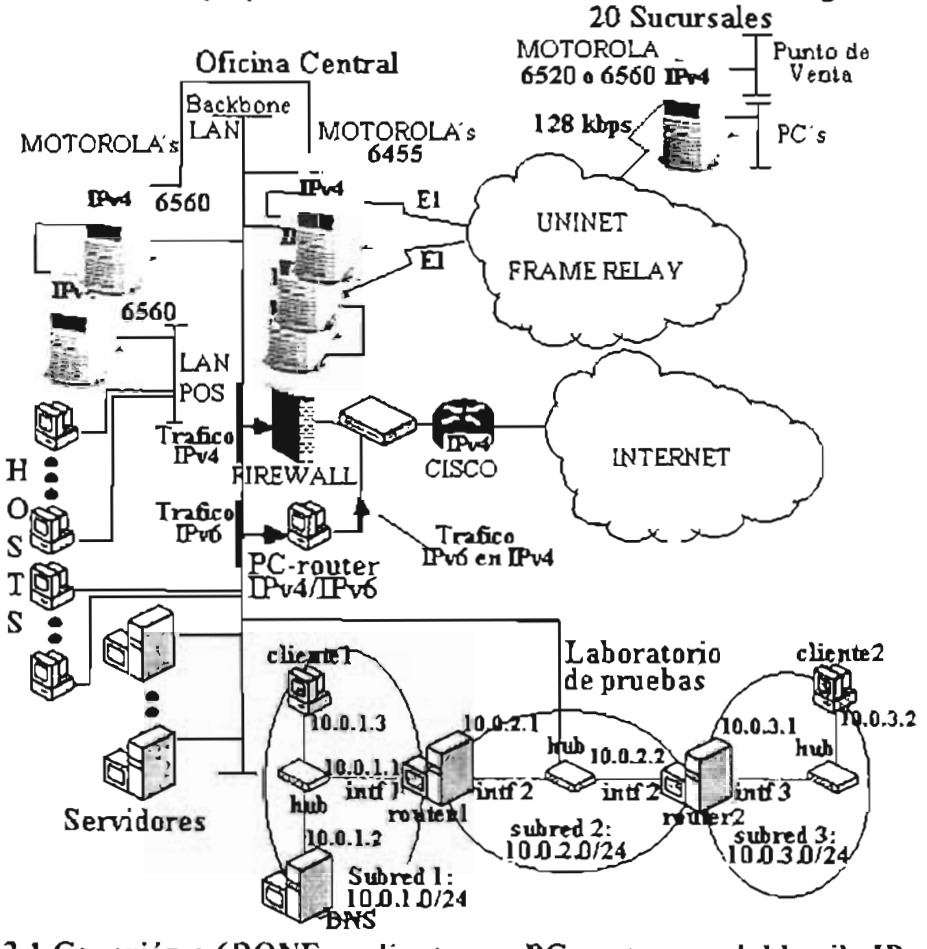


Fig. 6.3.1 Conexión a 6BONE mediante una PC-router con doble pila IPv4/IPv6

Con la PC-router habilitada con las dos pilas IPv4/IPv6, con dos tarjetas de red y una dirección IPv4 publica homologada en una de sus tarjetas de red podemos encapsular todo el trafico hacia IPv6 en IPv4, este trafico encapsulado llegara al 6BONE por medio del túnel estático que se configure con el ISP o PTLA o pNLA o con un túnel dinámico con lo cual el trafico puede ser dirigido a un router relay, en este caso el router relay sería el de Microsoft, este ultimo esquema con tunel dinámico 2002, con el router relay de Microsoft como gateway para nuestro trafico IPv6 se hicieron las pruebas correspondientes y funcionaron correctamente. Esta opción se puede implementar mediante una PC con dos tarjetas de red con el sistema operativo que se quiera utilizar como linux, BSD o Microsoft, en este caso se hizo esta prueba con una PC a la que se instalaron dos tarjetas de red y con sistema operativo Windows XP. El costo de esta implementación es el siguiente:

Equipo	Costo
PC soporte de S.O. para IPv6	$900.00 dls
Tarjeta de red Broadcom 10/100	$ 73.47 dls

El costo de la PC es un promedio de PCs de diferentes marcas con mejores características que una PC normal para que su desempeño como router sea adecuado.
En la propuesta de la migración hicimos notar que el firewall que protege a la red local del trafico de Internet no maneja aun IPv6, por lo que se tiene que actualizar el sistema operativo o cambiar el equipo. La actualización del software no se puede realizar ya que para este modelo el fabricante aun no ha liberado una versión de sofiware para IPv6. Netscreen libero un software con soporte de IPv6 el ScreenOS-5.0 para los modelos 204 en adelante y el 5XT, por lo que se tendría que cambiar el modelo actual ya sea por el 5XT o por el 204, en el caso del 5XT es un modelo mas abajo del 25 por lo que tendrá menos capacidad para el manejo de sesiones, túneles, políticas, etc. en cambio el 204 es aproximadamente cuatro veces mas poderoso que el 25, el costo de estos equipos es el siguiente:

Equipo	Costo
Firewall Netscreen-204	$10,000.00 dls
Firewall Netscreen-5XT	$2,000 dls. Aprox.

En este caso el modelo por el que se cambiaria seria el modelo 204.
El costo por actualización del hardware de los hosts, es decir el cambio de las PCs y servidores por maquinas con características minimas (procesador pentium IV a 3 GHz, 256 MB de RAM, 40 GB de disco duro) para soportar sistemas operativos que manejan IPv6 como Windows XP, (estas características son las requeridas por Microsoft para soportar la actualización de sistema operativo a Windows XP), tomamos XP ya que es el sistema operativo usado en la red propuesta, el costo de estas maquinas es el mostrado a continuación:

Equipo	Costo
PC sin sistema operativo	$650.00 dls
PC con SO incluido	$750.00 dls

Estos costos es un promedio de PCs de diferentes marcas que cumplen con las características requeridas.
Para el caso en que se propone un router adicional para el ruteo del trafico IPv6 interno a la red local, con capacidad de stack doble, se cotizo entre tres marcas para comparar costos, podría ser un cisco 2600 con dos tarjetas de red con IOS 12.2(2)T o más actual, nortel o un 3com equipos que ya manejan IPv6. nortel maneja IPv6 a partir de la versión 12.0 de la suite de protocolos BayRS, por su parte 3com partir de su versión de software 11.0 de sus routers Netbuilder II, el costo de poner cualquiera de ellos se muestra en la siguiente tabla:

Router	Costo
Cisco 2610XM 12.2(2)T	$ 2,695.00 dls
Nortel 12.0 BayRS	$ 7,100.00 dls
3com Netbuilder II 11.0	$ 2495.00 dls
3com Office Connect VPN Firewall	$ 397.3.00 dls.

En la red propuesta se cuenta todavía con algunos hubs que solamente trabajan a 10 Mbps, lo recomendable para IPv6 es que los equipos de interconectividad trabajen a 100 Mbps por lo que el costo de cambiar estos switches es el siguiente:

Equipo	Costo
SW 3com Super Stack 3 48 ptos. 10/100	$1,750.00 dls
SW 3com Superstack 3 4250T 48 ptos. 10/100	$898.3.00 dls
Switch Bay stack 470-48T, 48 ptos. 10/100	$3,604.00 dls
Switch Foundry FastIron 48 ptos. 10/100	$5,845.00 dls
Switch Passport 8648TXE 48 ptos. 10/100	$12,113.00 dls
Switch extreme Sumit48i 48 ptos. 10/100	$8,227.00 dls
Catalyst 3560 48 ptos. 10/100	$6,160.986 dls
Enterasys 48 ptos 10/100	$3,439.788 dls
Avaya Cajun 80 24 ptos. 10/100	$ 4,058.429 dls

El fabricante de los routers Motorola no tiene pensado a la fecha liberar una versión de software para que la infraestructura de ruteo de la red Lan pueda soportar IPv6.
Como tratamos de proponer esta migración con la idea de afectar lo menos posible la infraestructura que se encontraba funcionando y al mismo tiempo sin generar costos excesivos, el hecho de que Motorola no maneje IPv6 hace pensar como una opción proponer la sustitución de todos los routers Motorola por routers Cisco.
Sin embargo también se puede dejar la plataforma de routers Motorola actual hasta que termine su tiempo de vida útil y se decida cambiar, si no es que antes para lo cual entonces si se podría ya implementar la propuesta de sustituirlos por la marca Cisco.
Por lo que en caso de que se quisiera realizar el cambio de la infraestructura de routers Motorola por routers Cisco tenemos a continuación los costos de routers con las características necesarias para cumplir con las funciones que realizan actualmente los routers Motorola cotizados:

Equipo	Costo
Router Cisco 7206VXR/400 Central	$65,600.00 dls.
Router Cisco 2691 Remoto UNINET	$8,950.617 dls.
Cisco 2610XM respaldo D1 y D2	$ 4,503.954 dls
Cisco 2651XM V1	$9,510.306 dls.

Esta es una cotización especial ya que la infraestructura actual de routers motorola además de realizar el ruteo reciben los enlaces remotos por medio de puertos V35, G703, Rs232, y se comunican con los conmutadores por G703 también, por lo que estos routers son críticos ya que manejan tanto la voz como los datos.

6.4 COSTOS POR ACTUALIZACION DE SOFTWARE

Los costos en este aspecto pueden verse desde dos puntos de vista los costos por actualización del software que ya se maneja y los costos por software que se piense instalar.
En el primer aspecto nos referimos a lo siguiente, si por ejemplo la infraestructura de ruteo fuera ya toda Cisco. Cisco ya ha liberado sus versiones para IPv6, cuando se es cliente de Cisco probablemente se tenga una cuenta de usuario con la cual se pueden bajar libremente las nuevas versiones de IOS de la pagina web, por lo cual este aspecto no implica costo alguno.
En general para realizar las actualizaciones de la plataforma de PCS, servidores o routers o de las aplicaciones los fabricantes están o ya han desarrollado parches o versiones para IPv6 con posibilidad de bajarse libremente y probarse, por lo que en este aspecto no debería representar costos adicionales.
Para la red LAN propuesta podemos ver la los costos de actualización de software desde tres áreas principales:
Actualización de software en PCS.
Actualización de software en servidores.
Actualización de software en routers.
Actualización de aplicaciones.
En esta red LAN la actualización de la pila en las PCs no deberá tener ningún costo ya que todas las maquinas usan Windows XP que soporta IPv6 probado y funcionando correctamente en nuestro laboratorio de pruebas.
Por su parte los servidores de aplicaciones como Intranet, correo, antivirus, etc. trabajan con diferentes sistemas operativos como Linux, Windows NT, Windows 2000, servidores que actualmente los fabricantes de estos sistemas han liberado el parche para que manejen IPv6, o algunos ya lo tiene incluido el soporte para IPv6 como Linux.
La plataforma de routers que componen nuestra red es marca Motorola y a la fecha el fabricante no piensa siquiera en sacar una versión de prueba de software para IPv6. La actualización del software de los routers Motorola no se puede realizar, por lo que o se dejan trabajando estos equipos hasta el termino de su vida útil o se cambia toda la plataforma de Motorola a Cisco.
De este modo la actualización de software en los routers no implicara una fuerte inversión ya que solo se debera actualizar el router Cisco que maneja el trafico hacia Internet, el costo de la actualización de este software es de aproximadamente unos $300.00 dls.

En la parte inicial de la migración proponemos la actualización del IOS del Cisco 2600 que conecta la red local a Internet
Este equipo actualmente tiene el IOS 12.1T, deberá actualizarse a una versión 12.2 en adelante para soportar IPv4 e IPv6, el costo de la actualización del sistema operativo en un router cisco es el siguiente:

Router	Costo IOS
Cisco 2600	$300 dls.

Los equipos de computo como PCs y servidores necesitaran actualizarse a un sistema operativo que soporte IPv6, el costo de la actualización a Windows XP es el de la siguiente tabla:

Software	Costo
Windows XP professional	$ 204.00 dls
Windows XP home	$ 118.00 dls
Windows XP professional OEM	$180 dls
Windows XP home español OEM(venta con hardware)	$111 dls
Windows XP pro español	$ 245 dls
Windows 2003 Server	$ 204 dls.

6.5 EVALUACION ECONOMICA TOTAL

En base a los costos determinados en los puntos anteriores se obtuvo una aproximación del costo total de la actualización propuesta, como se muestra a continuación:

Concepto	Cantidad	Costo unitario	Costo total
Capacitación IPv6	2	$ 600 dls	$ 1,200.00 dls
Capacitación Windows XP	2	$ 610 dls	$ 1,220.00 dls
Capacitación Windows Server 2003	2	$ 610 dls	$ 1,220.00 dls
Firewall-204	1	$ 10.000 dls	$ 10.000.00 dls
PC con S.O. Windows XP	300	$ 750.00 dls	$ 225.000.00 dls
Switch Enterasys 48 ptos. 10/100	2	$3.439.788 dls	$ 6.879.576 dls
Router Cisco 7206VXR/400	1	$65.600.00 dls	$65.600.00 dls
Cisco 2610XM	2	$ 4.503.954 dls	$ 9007.908 dls
Cisco 2651XM	1	$9.510.306 dls	$9.510.306 dls
Cisco 2600 IOS 12.3	1	$ 300.00 dls	$ 300.00 dls
Costo total de la propuesta (oficina central)			$ 329,937.79 dls

Este costo total toma en cuenta el cambio de la plataforma de ruteo Motorola a Cisco debido a la falta de soporte de Motorola para IPv6. Este es un costo total aproximado ya que tomamos en cuenta para el calculo los elementos mas sobresalientes y por que como sabemos actualmente es difícil determinar un costo exacto del cambio a IPv6 ya que realmente sobre la marcha habrá detalles más específicos que surgirán e influirán en los costos totales.

Para el caso de las sucursales, tenemos las siguientes aproximaciones del costo de actualización.

Concepto	Cantidad	Costo unitario	Costo total
PCs con S.O. Windows XP	70	$ 750.00 dls	$52,500.00 dls
Router Cisco 2691	1	$8,950.617 dls	$8,950.617 dls
Costo total de la propuesta por sucursal			$ 61,450.617 dls.

En general la migración a IPv6 no debería verse como una gran inversión económica ya que como hemos mencionado el cambio de IPv4 a IPv6 debería verse no como un cambio drástico de tecnología sino como una actualización de protocolo, además por los requisitos impuestos por el IETF desde la propuesta de IPv6 se condiciono que el cambio fuera paulatino, independiente de cada nodo y con compatibilidad entre ambas versiones de IP, este cambio se puede ir realizando por etapas empezando por los puntos menos criticos y que implican menos costo en la realización de estos objetivos, los puntos mas delicados o de mayor inversión podrían dejarse para realizarse llegado el momento en que o se requieran cambios de equipos por obsolescencia o cuando se aplique alguna actualización planeada de equipos de comunicaciones, en estos momentos es cuando se puede aprovechar para realizar estos cambios, con lo cual se cumplen básicamente los objetivos de cumplir los objetivos trazados por cada empresa a la vez de que se esta preparado para los retos futuros en cuanto a la comunicación por Internet y para poder aprovechar las aplicaciones pueden realizar.

Esto no quiere decir que por esto se tenga que dejar dichos cambios para cuando lleguen esos momentos, cuando se esta en condiciones de implementar nuevas tecnologías este proceso podría empezar a realizarse desde ahora, la gran mayoría de las empresas han demostrado poco interés por IPv6, lo cual puede llegar a complicarse en el futuro cuando tal vez se tenga que realizar una migración precipitada que puede ser forzada por que en un momento dado la infraestructura de IPv6 sea mayoritaria o por un agravamiento de las limitaciones de IPv4, esto se podría evitar empezando desde ahora a realizar dicha migración, migración que aunque se realice poco a poco no afecta la comunicación con el resto del sistema.

Los costos de no empezar a migrara a IPv6 pueden ser mejor comprendidos en base a los problemas que se pueden llegar a experimentar conforme el uso de este progrese, así tenemos que el costo de permanecer en IPv4 y no migrara a IPv6 pueden ser:

- Perdida de la oportunidad de disfrutar el desarrollo de IPv6.
- Se generaran mayores desarrollos de negocios conforme IPv6 se desarrolle.
- Perdida de la oportunidad de disfrutar nuevas aplicaciones y servicios que se encuentran en cierto grado de madures gracias a que los routers y sistemas operativos soportan IPv6.

Realmente a la fecha aun es difícil determinar un costo monetario directo de lo que implica la migración a IPv6 como lo es igual de difícil determinar el costo que tendrá el no actualizarse a tiempo en IPv6.

Las recomendaciones que quisiéramos realizar están encaminadas mas que nada a ayudar, y apoyar la transición a IPv6:

- Que las empresas e industrias incrementen su presencia e interés en el proyecto de IPv6 lo que ayudara a que los desarrollos que ya se tienen actualmente sobre aplicaciones sistemas y redes de prueba de IPv6 puedan ser concretados en su mayoría para que llegado el momento de su adopción general la falta de funcionalidad correctamente probada no represente una limitación en su implementación.
- Las industrias y empresas deberían proporcionar una mayor difusión de IPv6 en el ámbito de producción como lo están haciendo actualmente un gran numero de instituciones educativas.
- La aplicación de mayores fomentos al desarrollo de nuevos servicios; redes y aplicaciones de IPv6 permitirán aprovechar de mejor forma la robustez de dicho protocolo lo que hará aun más justificable su implementación a nivel general.
- Particularmente debería haber una mayor promoción para que se propicie la implantación de IPv6 en las empresas, lo que puede ayudar a un despegue mas rapido de IPv6.
- La exploración y apoyo a nuevos proyectos que estudien aplicaciones sobre las nuevas características de IPv6 deberían ser implementados en instituciones, empresas, industrias y gobiernos.

7. CONCLUSIONES

La transición y coexistencia a IPv6 es un proceso que puede empezar a realizarse lentamente y por etapas lo que permitirá una familiarización paulatina con IPv6 así como la seguridad de que su funcionamiento ha sido probado.
Aunque no se percibe una problemática insalvable con IPv4 en un corto o mediano plazo la transición podría empezar a realizarse ya, tal vez aprovechando los planes de mantenimiento o actualización programados que usualmente se proyectan en las redes, para que de esta manera el impacto en los diversos aspectos técnicos, económicos y funcionales principalmente no sea tan fuerte.
IPv6 es un protocolo apropiado para enfrentar los problemas de escalamiento de IPv4. IPv6 proporciona mecanismos flexibles para la transición de las redes actuales. Al permitir gran cantidad de direcciones jerárquicas permitirá el soporte de los nuevos mercados de aplicaciones (aplicaciones en tiempo real, seguridad de extremo a extremo, autoconfiguración, movilidad, etc.) y el crecimiento de Internet al proveerla de nuevas capacidades de enrutamiento más eficientes. IPv6 trabajara eficientemente tanto en redes de alta velocidad como en redes de ancho de banda bajo.
Aparte de las nuevas ventajas de IPv6 la introducción del protocolo puede dar a las empresas la oportunidad de rediseñar las redes que satisfagan nuevas necesidades y que se basen en las lecciones aprendidas con IPv4. Probablemente se presenta un panorama de inversiones fuertes pero que a largo plazo resultara en grandes beneficios.
El análisis de las características de IPv6 y las estrategias que se pueden implementar para su adopción permiten vislumbrar que IPv6 es una tecnología madura que se encuentra lista para ser usada en modo nativo en redes de producción. La introducción de IPv6 en producción esta lista, esto lo podemos afirmar en base a las pruebas realizadas, las facilidades de migración y coexistencia existentes, así como la cantidad enorme de aplicaciones, sistemas operativos y hardware que lo soportan.
La gran mayoría de fabricantes de equipos de comunicaciones, de software, instituciones educativas están contribuyendo con el desarrollo de equipos, software y pruebas con IPv6.
Gran parte de las aplicaciones que se están desarrollando para trabajar con IPv6 están disponibles gratuitamente por sus creadores junto con su código abierto y además existe un gran intercambio de los desarrollos sobre IPv6 por Internet.
La conectividad a la red IPv6 y delegación de prefijos es proporcionada únicamente por instituciones educativas, de investigación o intermediarios, mientras que no se visualiza cuando proporcionaran estos servicios los grandes ISPs.
Probablemente en los inicios de implantación de IPv6 no se puedan explotar o apreciar todas las mejoras de sus nuevas características debido a la coexistencia que deberá tener con IPv4 como parte del proceso de migración, pero conforme se avance en el proceso de la implantación además de las mejoras que tiene con respecto a IPv4 propiciara el desarrollo de muchísimas nuevas aplicaciones y de las que estaban en espera de tener condiciones adecuadas para su desarrollo.

En base a las pruebas realizadas, la teoría, las características y funcionamiento de IPv6, podemos decir que IPv6 tiene muchas ventajas y mejoras con respecto a IPv4.
La coexistencia entre IPv6 e IPv4 funciona sin ningún problema. Los equipos que trabajan con IPv6 pueden comunicarse perfectamente con los equipos que solo

trabajan con IPv4, y estos a su vez no presentan algún problema para manejar, aceptar y dejar pasar el trafico de IPv6 previamente encapsulado con un encabezado IPv4.

Con las pruebas realizadas podemos afirmar que las características y funcionamiento de IPv6 hacen a este protocolo mejor que el protocolo IPv4, sobre todo para las nuevas aplicaciones que se están desarrollando para funcionar sobre Internet, todas esas nuevas aplicaciones estarán basándose en algunas de las características de IPv6 como su amplio direccionamiento jerárquico, la seguridad intrínseca del protocolo, la movilidad, la calidad de servicio, entre otras.

Durante las pruebas también pudimos darnos cuenta que las condiciones están dadas para que la actualización masiva a IPv6 se pueda dar en cualquier momento, ya que anteriormente una de las principales preocupaciones era la actualización de las pilas en ruteadores, nodos y aplicaciones, pero hoy la gran mayoría de ruteadores, sistemas operativos, así como las aplicaciones soportan la pila IPv6 nativamente o por lo menos existen parches para habilitar dicho soporte.

Asimismo las pruebas nos permitieron comprobar que la disponibilidad de IPv6 se encuentra lista y funcionando correctamente en muchas plataformas y equipos. En el caso de la red LAN propuesta cuyo sistema operativo base es Windows XP, se pudo comprobar que este sistema funciona correctamente con IPv6 implementando la gran mayoría de las características de IPv6, como el manejo de los diferentes tipos de direcciones IPv6 (compatibles, de enlace local, de sitio local, temporales, 6to4, etc.), el uso de túneles ya sea dinámicos o estáticos, el manejo de la seguridad. Pudimos comprobar que el servidor DNS de Windows 2003 Server trabaja perfectamente para la resolución de nombres en direcciones IPv6, sucede lo mismo con los servidores DNS de Internet.

Asimismo pudimos comprobar que ya existe en Internet una gran base de equipamiento y facilidades para probar y trabajar con IPv6 como los routers relay, proveedores de túneles brokers, sitios IPv6, etc.

Es un hecho que IPv6 mejora la velocidad de la comunicación entre los equipos a nivel de red, ya que gracias al formato de su encabezado simplificado el procesamiento de los paquetes IPv6 por parte de los equipos de ruteo disminuye puesto que al tener menos campos el encabezado del paquete, el tiempo de procesamiento de menos campos deberá ser menor para cada paquete. Esta característica de IPv6 aunada a que ciertas funciones que anteriormente tenían que ser realizadas en cada router por el que circulaba un paquete de IPv4 han sido eliminadas, como es el caso de la segmentación que ahora solo la realizan prácticamente los extremos que se están comunicando, todo esto ayudara a que la retransmisión de cada paquete que realicen los ruteadores sea más rápida y eficiente.

A nivel de enlace el uso de IPv6 ayudara a que el performance y por tanto la velocidad de comunicación entre los hosts aumente puesto que nuevamente las características de IPv6 ayudaran a esto ya que con la eliminación del proceso de broadcast usado en IPv4 para localizar hosts la red no será inundada con paquetes a todos los hosts que la integran, por lo que el uso de multicast dirigido ayudara a que un menor numero de paquetes sean mandados a la red cuando se desea establecer la comunicación con algún nodo, gracias al uso de direcciones autoconfiguradas con el formato EUI-64, así el multicast podrá buscar todos los nodos destino con los últimos 4 octetos de la dirección destino, lo que ayudara a que solamente el nodo destino procese el paquete dirigido a el, además un nodo puede ser configurado para que deseche el paquete multicast que no sea dirigido hacia él, no así los

paquetes de broadcast los cuales interrumpen momentáneamente el funcionamiento de cualquier nodo al que llegan. Por todo esto IPv6 mejorara por lo menos al doble la velocidad y desempeño de las redes.
El uso de IPv6 definitivamente permitirá aumentar la seguridad de la información ya que con la obligatoriedad de IPsec como algo intrínseco al protocolo, ya no se dependerá del uso de la seguridad implementada en capas superiores únicamente o mediante algún sistema independiente, por lo que desde el nivel de red se podrá implementar dicha seguridad sin ningún problema. Las pruebas realizadas nos permitieron comprobar que la seguridad de IPv6 funciona bien y es factible de implementar desde los mismos nodos finales de la comunicación.

Se necesita dar mas de difusión y apoyo a la instalación de este nuevo protocolo en los sistemas de comunicaciones reales o de producción, ya que es evidente que solamente las instituciones académicas y fabricantes han realizado y siguen realizando pruebas de IPv6, aunque se han realizado las pruebas en diferentes ambientes, en distintas plataformas de hardware y software, me parece que esta faltando su implementación a nivel de sistemas en producción, implementación que puede realizarse por etapas, lo que a su vez ayudara a que diferentes sectores empiecen a realizar la parte que les toca como por ejemplo los carriers, los cuales son un sector que no muestra mucha actividad respecto al tema.
Muchos ISPs y empresas no pareen tener mucho interés o un plan de transición a IPv6, aunque muchas instituciones han comenzado a realizar una introducción acelerada de IPv6 y diversos países, principalmente los asiáticos han empezado la transición a tal grado que ya ofrecen servicios comerciales con IPv6.
Se deben de empezar a realizar mas pruebas de interoperabilidad a niveles comerciales para continuar y extender las pruebas sobre IPv6, lo que nos ayudara a tener los elementos necesarios para en su momento poder seleccionar los mejores escenarios o métodos de transición y coexistencia que se apeguen o faciliten las tareas involucradas en el proceso de transición.

Como conclusión general la conectividad con IPv6 funciona de manera correcta, ya que no se presenta algún problema de conectividad con las utilerías de diagnostico básicas, con las pruebas realizadas IPv6 funciono perfectamente, además IPv6 es perfectamente compatible con IPv4 así como con los equipos que solo manejan IPv4, las pruebas realizadas y resultados obtenidos y capturados nos permiten ver claramente que su implementación no debe tener mayor problema.
En general podemos afirmar con toda seguridad que las condiciones están dadas y probadas para realizar una migración de IPv4 a IPv6 con la confianza de que el funcionamiento de las redes podrá continuar normalmente.
La migración a IPv6 puede ser implementada nodo por nodo usando la autoconfiguración para beneficiarse desde un principio de las ventajas de IPv6, al mismo tiempo que se mantiene la comunicación con IPv4.

APÉNDICE A

Resumen de pruebas realizadas con diferentes esquemas del laboratorio de pruebas con IPv6.
Este es un resumen de todas las pruebas que se realizaron con IPv6, en todas estas pruebas se capturo el trafico generado con el software Ethereal, el cual permite observar en forma detallada los campos de los datagramas IPv6.

Se implemento un laboratorio de pruebas con 5 maquinas conectadas de tal manera que se tenían 3 subredes IPv4 diferentes, 2 de esas maquinas funcionaban como routers, otras dos como clientes y la restante como servidor DNS. Todas las maquinas podían trabajar con IPv4 e IPv6. El esquema del laboratorio inicial es el mostrado en la Fig. A.1

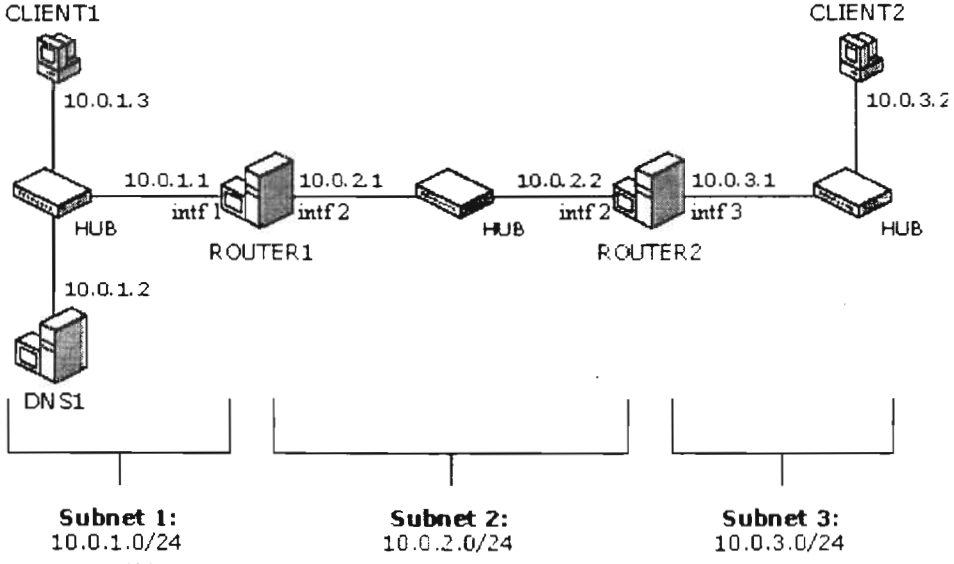


Fig. A.1 Esquema inicial del laboratorio de pruebas

Los hosts del laboratorio fueron configurados inicialmente con un direccionamiento IPv4 privado.
Como se puede ver se tiene una subred 1 10.0.1.0 (IPv4) o FEC0:0:0:1::/64 (IPv6) formada por los hosts: cliente1 (10.0.1.3), DNS (10.0.1.2) y router1 (10.0.1.1).
Se tiene una subred 2 10.0.2.0 (IPv4) o FEC0:0:0:2/64 (IPv6) formada por las interfaces de los routers: router1 (10.0.2.1) y router2 (10.0.2.2)
Y una tercera subred 10.0.3.0 (IPv4) o FEC0:0:0:3::/64 formada por: el router 2 (10.0.3.1) y cliente2 (10.0.3.2)
A los hosts llamados routers 1 y 2 se les instalo un tarjeta Ethernet PCI adicional a la que tiene cada maquina de fabrica y se les habilito el ruteo desde el sistema operativo para que pudieran redireccionar el trafico de una tarjeta de red a la otra.
Los 2 clientes (1 y 2) trabajaron con el sistema operativo Windows XP.
Al servidor DNS se le instalo el sistema operativo Windows 2003 Server, además del sistema operativo Windows XP que ya tenia la maquina, pero básicamente se hicieron las pruebas con Windows 2003 Server que nos permite configurar los diferentes roles de servidor de la maquina.

Los routers 1 y 2 tenían instalados ambos sistemas operativos Windows XP y Windows Server 2003.
El sistema operativo Windows Server 2003 incluye un software de monitoreo de red con el cual inicialmente se empezó a capturar el trafico generado por las pruebas. El problema con este software de monitoreo de red es que detecta el trafico IPv6 pero no muestra explícitamente las direcciones IPv6 en su formato hexadecimal separado por dos puntos o forma normalizada, únicamente indica que se trata de trafico IPV6, por lo cual no se uso para terminar todas las pruebas realizadas.
En algunas pruebas se inserto un router que solo trabaja con IPv4, un router Motorola 6520 con dos tarjetas de red. Se uso este router para probar la conectividad de direcciones que hacen encapsulamiento de IPv6 con encabezado IPv4, esto con el fin de comprobar que funciona el encapsulamiento y que dicho encapsulamiento es transparente para equipos que solo manejan IPv4 como es el caso del router Motorola 6520, es decir necesitábamos verificar que este tipo de equipos dejan pasar el trafico IPv6 encapsulado sin ningún problema.
También se conecto la red del laboratorio a Internet IPv4 con un router CISCO que también solo trabaja con IPv4, la idea de conectar el laboratorio de pruebas a Internet era que las maquinas con direcciones IPv6 tuvieran acceso hacia el Internet, para probar el encapsulamiento de IPv6 sobre IPv4 en el ambiente real de Internet.
Se usaron dos tipos de conexiones a Internet, un enlace dedicado contratado con UNINET de 2 Mbps con un bloque de direcciones publicas homologadas fijas y un enlace de prodigy infinitum contratado con Telmex de 512 kbps.
Se instalo en cada una de las maquinas el software Ethereal para capturar el trafico. Este software detecta el trafico IPv6 y muestra las direcciones IPv6 en su forma conocida, es decir con el formato normalizado de dos octetos hexadecimales separados por dos puntos.
En cada prueba realizada se capturo la pantalla del software ethereal y se anexo esta, a la prueba realizada, también en algunos casos se anexo el texto plano mostrando el trafico en forma decodificada (muestra de cada una de las tramas que componen al paquete), el texto plano solo se anexo como muestra en algunos casos ya que es demasiada información para ser presentada en un texto escrito.

- **Herramientas de prueba de conectividad**. Para todas las pruebas se usaron las utilerías o comandos de prueba mas conocidas que se usan en IPv4 para probar la conectividad, esto con la finalidad de probar la compatibilidad y funcionamiento de IPv6. Por lo tanto se probaron los diferentes esquemas del laboratorio con: PING, TRACERT, PATHPING, TELNET, FTP, HTTP, y se verifico que se pudieran resolver nombres a direcciones IPv6 con registros AAAA. Estas utilerías o herramientas de prueba que se usaron son las que trae el sistema operativo Windows XP y 2003 Server. El PING, el Tracert y el PATHPING se corrieron desde el prompt de sistema del modo de comandos de Windows, para usar Telnet y FTP se levantaron los servicios que incluyen el SO Windows de Telnet y FTP. Para usar el http desde la barra de direcciones URL del navegador Internet Explorer se teclearon nombres de direcciones que deberían ser traducidas a direcciones IPv6 por medio de la búsqueda en el servidor DNS (el navegador Internet Explorer aun no soporta que se le indique en su barra de direcciones la dirección de un host entre corchetes en el formato de octetos hexadecimales separados por dos puntos).

Las pruebas que se hicieron con este laboratorio en forma general fueron las siguientes:

- **Se instalo y configuro el servidor DNS para resolver nombres de hosts en direcciones IPv6.**
- **Pruebas de conectividad IPv6 entre nodos que se encuentran en la misma subred de una red IPv6. Direcciones link local (prefijo FE80).**
  Se capturo el trafico generado durante las pruebas de comunicación entre hosts con direcciones de link local (Prefijo FE80). Este tipo de direcciones se configuran automáticamente cuando se instala IPv6 en los hosts, estas direcciones no se pueden usar para comunicar hosts que se encuentran en subredes diferentes, ya que su ámbito es local a la subred en la que se encuentran. Pruebas con estas direcciones solamente se pueden hacer entre hosts que están en la misma subred, es decir para la subred 1 (Fig. A.1) solamente se pueden hacer pruebas del cliente1 al DNS y viceversa, del cliente1 al router1 y viceversa, del dns al router1 y viceversa. Para la subred 2 solamente se pueden hacer pruebas del router1 al router2 y viceversa. Para la subred 3 del router2 al cliente2 y viceversa.
- **Pruebas de conectividad con seguridad (ESP y AH) IPv6 entre nodos que se encuentran en la misma subred de una red IPv6. Direcciones link local (prefijo fe80).**
  Para las direcciones link local (FE80) se configuraron los hosts que se encontraban en las mismas subredes para aplicaran la seguridad ESP y AH a las pruebas realizadas.
- **Pruebas de conectividad IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv6. Direcciones site local (prefijo FEC0).**
  Se configuro en las maquinas una estructura de ruteo estático para que por anunciamiento de los prefijos por parte de los routers, los hosts autoconfiguren direcciones IPv6 con prefijo de site local (prefijo FEC0). El objetivo de esta prueba además de probar el anunciamiento de prefijos por parte de los routers es permitir la comunicación con IPv6 entre subredes diferentes de una red LAN, es decir (Fig. A.1) que los hosts se puedan comunicar de extremo a extremo del laboratorio aunque estén en subredes diferentes, es decir que el cliente 1 se pueda comunicar con el cliente 2 y viceversa y que de esta manera todos los hosts ya se puedan ver con todos los demás, no importando en que subred se encuentren.
- **Pruebas de conectividad IPv6 por resolución de nombres entre nodos que se encuentran en diferentes subredes de una red IPv6. Direcciones site local (prefijo FEC0).**
  Se configuraron registros del tipo A y AAAA en el servidor DNS para que resolviera nombres de hosts en direcciones IPv4 e IPv6 de site local.
- **Pruebas de conectividad con seguridad IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv6. Direcciones site local (prefijo FEC0).**
  Para las direcciones de site local (FEC0) se configuro un esquema de seguridad con los protocolos ESP y AH para asegurar el trafico de extremo a extremo desde el cliente 1 al cliente2.
- **Túnel ISATAP. Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv4. Direcciones ISATAP (FE80::5EFE:w.x.y.z).**

Se implemento una estructura de comunicación entre los hosts de una red IPv6 y los hosts de una intranet IPv4-only con direcciones ISATAP (FE80::5EFE:w.x.y.z). Con este tipo de direcciones los hosts de la subred IPv6 encapsulan el trafico IPv6 con encabezados IPv4 para comunicarse con los hosts de la red IPv4.

- **Túnel automático v4-compatible. Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv4. Direcciones v4-compatibles (::w.x.y.z).**
  Se hicieron pruebas con direcciones IPv4-compatibles (Direcciones del tipo ::w.x.y.z), estas son direcciones que cada host autoconfigura al tener una dirección IPv4 publica en su interfaz ethernet, este tipo de direcciones encapsulan automáticamente el trafico IPv6 con un encabezado IPv4.
- **Túnel automatico 6to4. Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 temporales (prefijo 3FFE).**
  Se hicieron pruebas con direcciones globales temporales (prefijo 3FFE). Este tipo de direcciones temporales se autoconfiguran cuando se configura una estructura de ruteo estático con estos prefijos además de que se deben tener direcciones IPv4 publicas y habilitar ICS (Internet Connection Sharing) para compartir la conexión a Internet.
- **Pruebas de conectividad IPv6 por resolución de nombres entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 temporales (prefijo 3FFE).**
  Se configuraron registros del tipo AAAA en el servidor DNS para que resolviera nombres de hosts en direcciones IPv6 temporales (3FFE).
- **Tunel automatico 6to4. Pruebas con direcciones IPv6 globales que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 o globales (prefijo 2002).**
  Se hicieron pruebas con direcciones 6to4 (Prefijo 2002), con este tipo de direcciones se puede tener una conexión real a y desde Internet. Este tipo de direcciones también encapsulan el trafico IPv6 con un encabezado IPv4, así de esta forma se puede tener comunicación hacia Internet. Con este tipo de direcciones se implementaron diferentes esquemas para probar la conectividad de este tipo de direcciones en ambientes de pruebas simulados por el laboratorio y para realizar conexiones reales de las subredes del laboratorio a Internet.
- **Pruebas de seguridad con direcciones IPv6 globales que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 o globales (prefijo 2002).**
  Se construyeron dos esquemas para implementar la seguridad en los cuales se hizo pasar el trafico asegurado con el protocolo ESP por un túnel de encapsulamiento AH. El primero de los esquemas solo aseguraba el trafico del cliente 1 al router2 y el segundo aseguraba el trafico de extremo a extremo, es decir del cliente 1 al cliente2.
- **Pruebas de conectividad IPv6 por resolución de nombres entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 o globales (prefijo 2002).**
  Se configuraron registros del tipo AAAA en el servidor DNS para que resolviera nombres de hosts en direcciones IPv6 globales (2002).

Esquemas implementados para realizar las pruebas:

Pruebas de trafico IPv6 entre nodos que se encuentran en la misma subred de una red IPv6. Direcciones link local (prefijo fe80).

Para pruebas con este tipo de direcciones el esquema original del laboratorio se vería de la forma ejemplificada en la Fig. A.2:

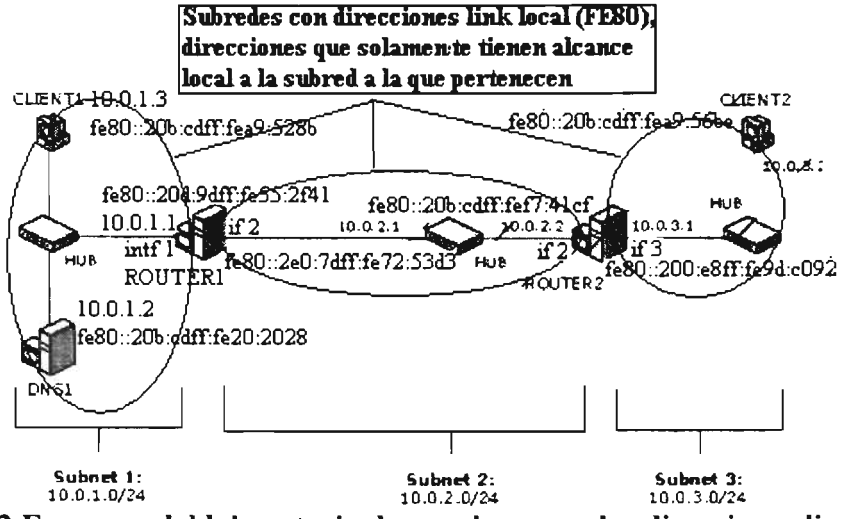


Fig. A.2 Esquema del laboratorio de pruebas para las direcciones link local.

Debido a que las direcciones de link local (fe80) son de ámbito local encerramos en círculos los hosts (Fig. A.2) que se pueden comunicar entre ellos con direcciones de este tipo.

Estas direcciones se autoconfiguran en cada host al ser instalada la pila IPv6.

Ya que las direcciones de link local son de ámbito local se hicieron pruebas con estas direcciones (ping, tracert, pathping, telnet, ftp, http, seguridad AH y ESP) entre hosts que se encontraban en la misma subred como muestra cada circulo en la Fig. A.2.

Pruebas de conectividad con seguridad (ESP y AH) IPv6 entre nodos que se encuentran en la misma subred de una red IPv6. Direcciones link local (prefijo fe80).

Para las pruebas de seguridad con direcciones link local (FE80) el esquema es el mostrado en la Fig. A.3:

Como se observa en la Fig. A.3 se configuraron políticas de seguridad y asociaciones de seguridad entre los hosts que pertenecen a la misma subred para probar la comunicación entre ellos con direcciones de link local usando seguridad IPSec con los protocolos ESP y AH

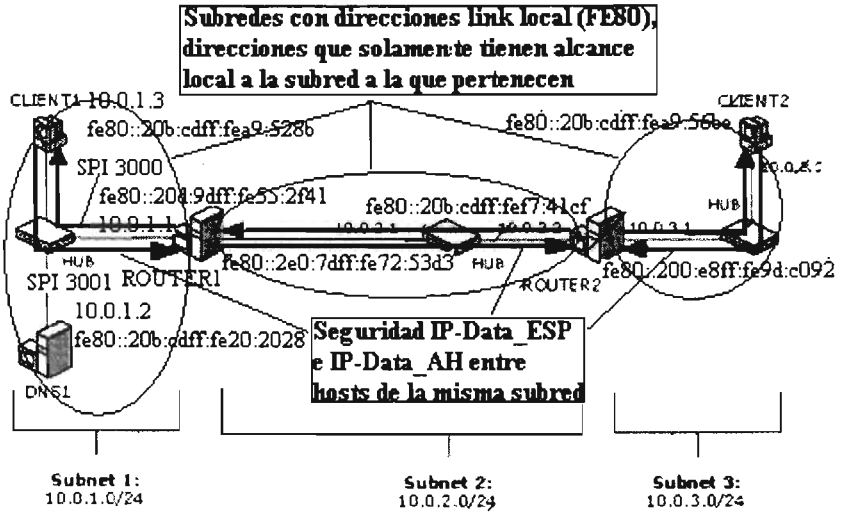


Fig. A.3 Esquema del laboratorio de pruebas con seguridad entre hosts que usan direcciones link local.

Pruebas de conectividad IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv6. Direcciones site local (prefijo FEC0).

El esquema para estas pruebas es el mostrado en la Fig. A.4. Para estas pruebas se configuro una estructura de ruteo estática en cada uno de los routers, los cuales anuncian estas rutas y sus prefijos provocando de esta manera que cada host autoconfigure direcciones de site local (prefijo FEC0) en base a los prefijos que le son anunciados.

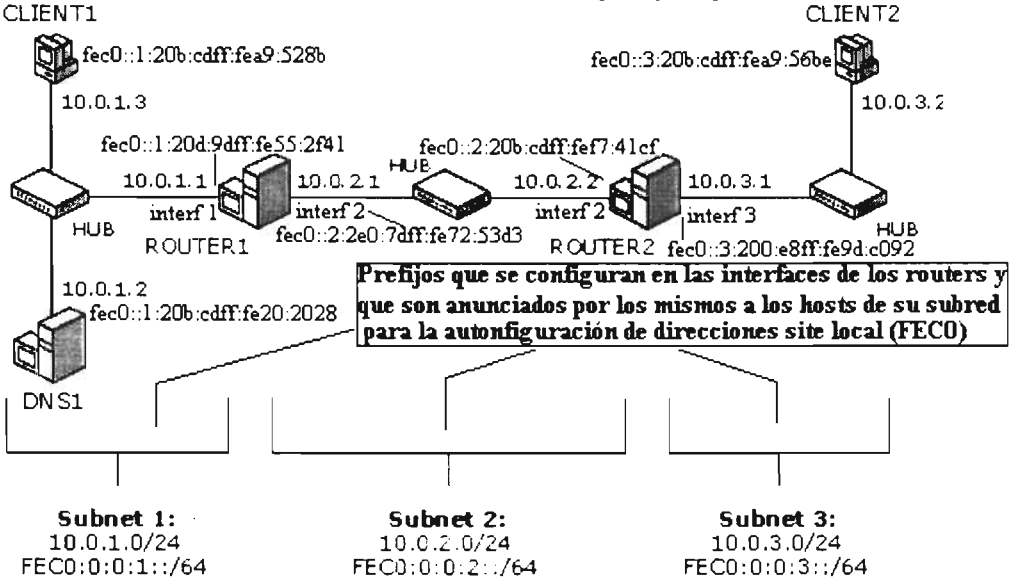


Fig. A.4 Esquema del laboratorio de pruebas con direcciones de site local.

Pruebas de conectividad con seguridad IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv6. Direcciones site local (prefijo FEC0).

Como las direcciones de site local (FEC0) son de ámbito intrasubred, para hacer pruebas de seguridad se configuro la seguridad ESP y AH de extremo a extremo es decir de cliente 2 a cliente 1 como muestra la Fig. A.5.

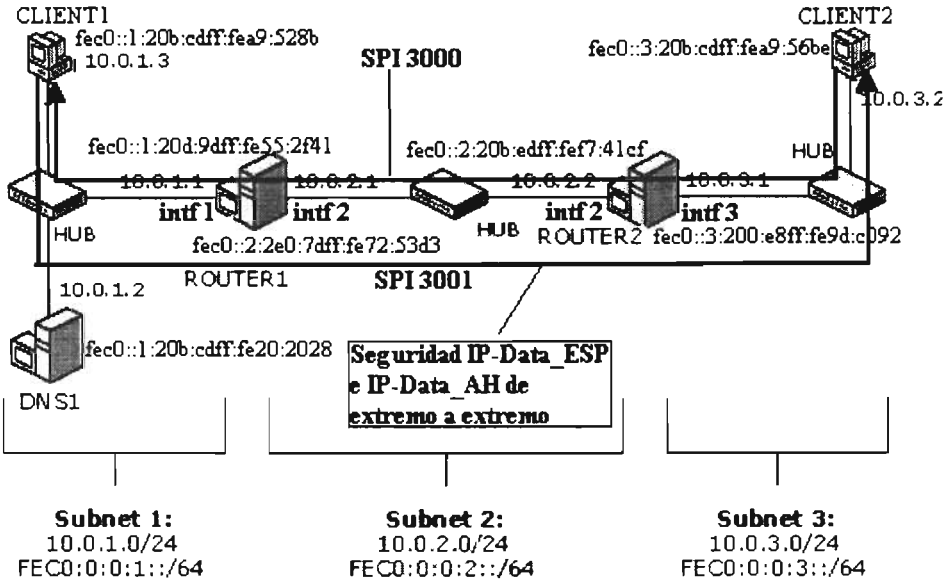


Fig. A.5 Esquema de pruebas con seguridad de la comunicación de extremo a extremo con direcciones site local

Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv4. Direcciones ISATAP (FE80::5EFE:w.x.y.z).

Se hicieron pruebas con las direcciones ISATAP en la forma fe80::5efe:w.x.y.z, esta es la forma por default en que se autoconfiguran en la interfaz isatap de cada nodo, estas pruebas nos ayudaron a probar el encapsulamiento con este tipo de direcciones, como muestra la Fig. A.6.

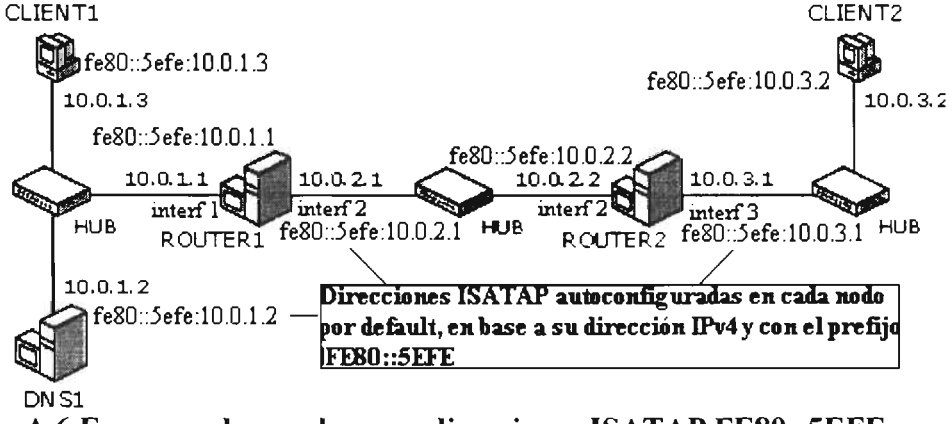


Fig. A.6 Esquema de pruebas con direcciones ISATAP FE80::5EFE:w.x.y.x

Para probar la aplicación de estas direcciones en la comunicación de una subred IPv6 con una Intranet IPv4-únicamente se uso el esquema de la Fig. A.6.

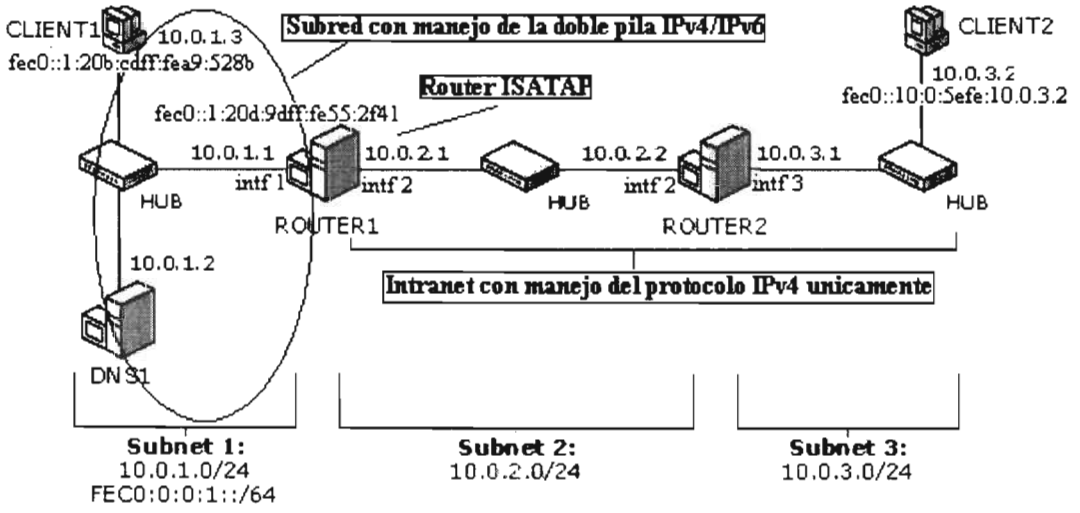


Fig. A.6 Esquema de comunicación entre una Intranet IPv4 y una subred IPv6 con direcciones ISATAP.

En este esquema lo que se hizo fue dividir o separar lógicamente el laboratorio en dos partes, una parte con conectividad IPv6-unicamente y una parte con conectividad IPv4-únicamente. A la subred 1 (compuesta por el cliente 1, el DNS y el router 1) se le configuro una estructura de ruteo con prefijo de site local, mientras que a las subredes 2 y 3 se les configuro únicamente un direccionamiento con IPv4 y a las interfaces de los routers (int2 del router2, intf 2 e intf3 del router2) que pertenecen a la Intranet con conectividad IPv4-únicamente se les deshabilito el anunciamiento y redireccionamiento (advertising y forward).

La idea con este esquema es que el host cliente2 que se encuentra en una subred IPv4-únicamente pueda comunicarse con el host cliente1 que se encuentra en una subred IPv6 y viceversa

Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes subredes de una red IPv4. Direcciones v4-compatibles (::w.x.y.z).

El esquema para probar este tipo de direcciones es el de la Fig. A.7.

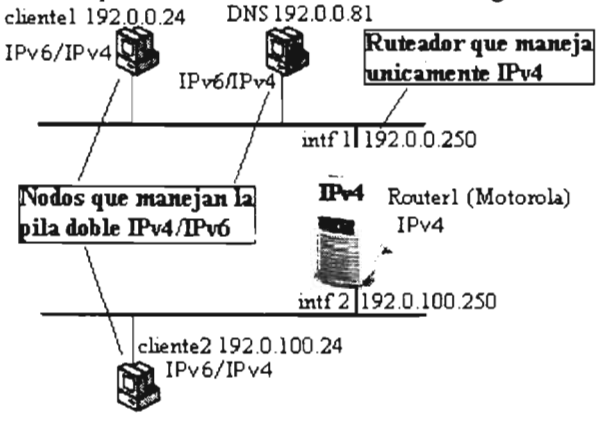


Fig. A.7 Esquema de pruebas con direcciones v4-compatibles.

Cuando a un host con manejo de IPv6 se le configuran direcciones IPv4 publicas, este automáticamente autoconfigura direcciones v4compatibles en su interfase, este tipo de

direcciones serán usadas para encapsular el trafico IPv6 con encabezados IPv4. Se probo este tipo de direcciones con el esquema de la figura A.7 para verificar que los hosts IPv6 pudieran comunicarse al tener en medio un equipo que solamente maneja IPv4, a la vez que pudimos observar en el router el trafico que se generaba con las peticiones de los hosts.

Pruebas con direcciones IPv6 que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 temporales (prefijo 3FFE).

El esquema usado para probar estas direcciones fue el de la Fig. A.8.

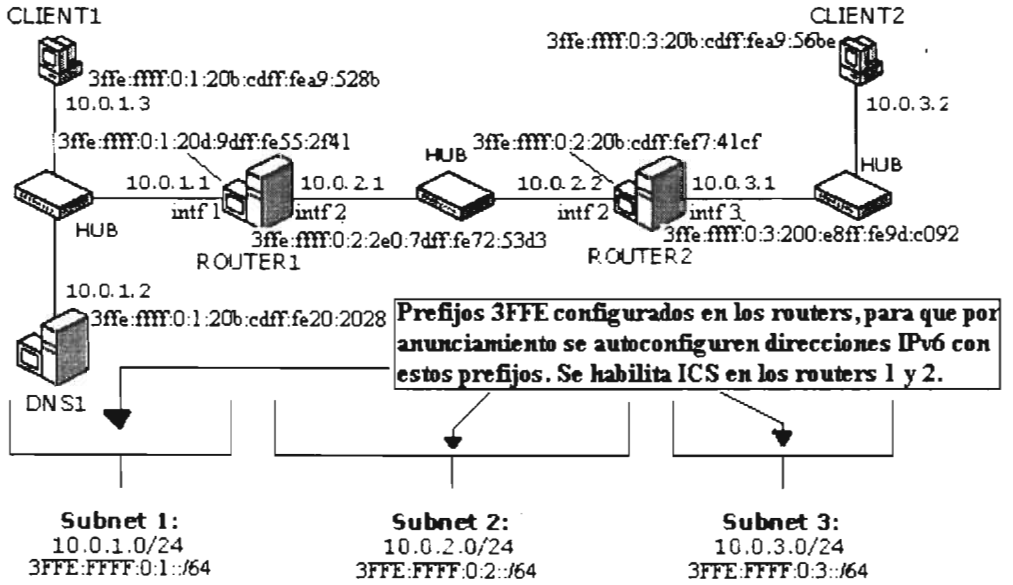


Fig. A.8. Esquema de pruebas con direcciones temporales 3FFE.

Este es el mismo esquema de las direcciones de site local solamente que ahora en la infraestructura de ruteo estática configurada en los routers se usaron prefijos 3ffe los cuales al ser anunciados por los routers autoconfiguran direcciones con ese prefijo.

Pruebas con direcciones IPv6 globales que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet. Direcciones 6to4 o globales (prefijo 2002).

En estas pruebas se usaron varios esquemas para realizar diferentes tipos de pruebas, con estas direcciones se pueden realizar conexiones como muestra la Fig. A.9.

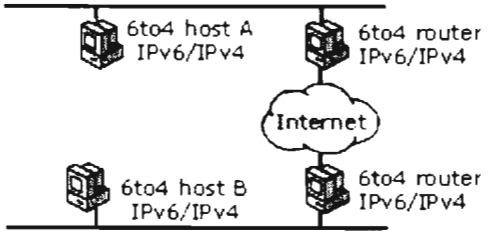


Fig. A.9 Esquema de pruebas de comunicación a través de Internet con direcciones 6to4.

Esquema con direcciones IPv4 publicas de la misma subred en las interfaces 2 de los router 1 y 2 (192.0.0.81 192.0.0.81), con Internet compartido.

Ya que la idea de estas direcciones como muestran la Fig. A.9 es pasar trafico IPv6 a través del Internet IPv4, primeramente checamos en nuestro esquema de laboratorio que los hosts se comunicaran con este tipo de direcciones como muestra la Fig. A.10.

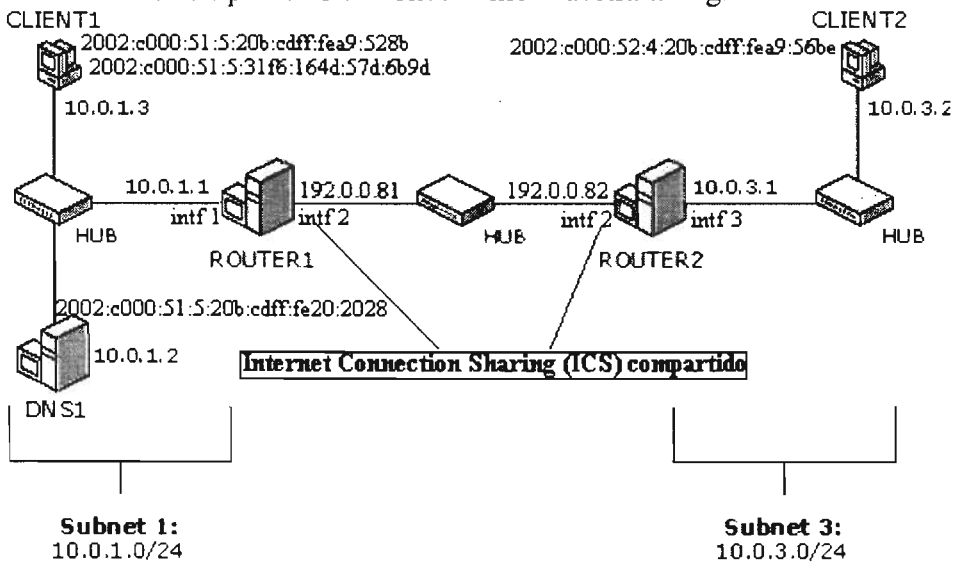


Fig. A.10. Esquema de pruebas con direcciones 6to4 localmente.

En este primer esquema 6to4 a las interfaces de los routers que pertenecen a la subred 2 se les configuro una dirección IPv4 publica (192.0.0.81 para el router1 y 192.0.0.82 para el router 2) además de que se compartió en esas interfaces el Internet (ICS) hacia las interfaces internas o privadas.

Con este esquema se pretendía probar la conectividad extremo a extremo con direcciones 6to4. Como los routers 1 y 2 tienen direcciones IPv4 publicas (pertenecientes a la misma subred IPv4), se les habilito la característica 6over4 y se les habilito ICS (Internet Connection Sharing) con lo cual la pila IPv6 autoconfigura direcciones 6to4 en base a estas direcciones IPv4 publicas y publica sus prefijos hacia los hosts que ese encuentran en la parte interna de la misma subred del router. En este caso el hub intermedio que interconecta a las interfaces de los routers representa el Internet IPv4. Y con este esquema se corrieron las pruebas de conectividad de extremo a extremo (cliente1-cliente2) con direcciones globales (2002).

Esquema con direcciones IPv4 publicas de diferente subred en las interfaces 2 de los router 1 y 2 (192.0.0.147 192.0.100.63) conectadas por medio de un router que solamente maneja IPv4, con Internet compartido.

A las interfaces de los router 1 y 2 se les cambiaron sus direcciones publicas para que no pertenecieran a la misma subred, debido a esto ya no se pueden interconectar por medio de un simple hub para lo cual se inserto un router que solamente maneja IPv4 para interconectar las dos subredes IPv4 publicas de los routers, como muestra la Fig. A.11.

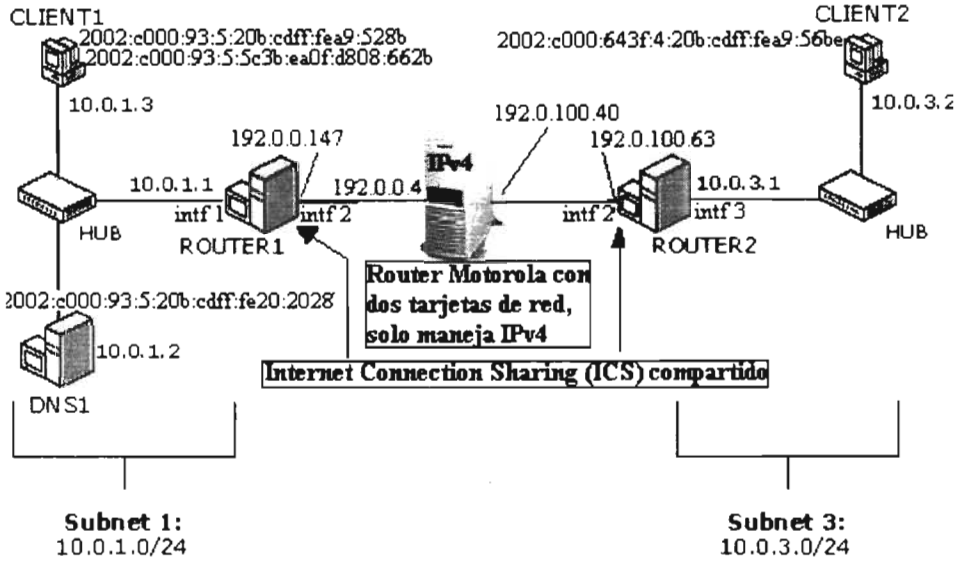


Fig. A.11. Esquema de pruebas con direcciones 6to4 localmente.

La idea de este esquema es probar la conectividad de extremo a extremo con direcciones 6to4 pero pasando por un equipo que solamente maneja IPv4 y así comprobar el encapsulamiento IPv6 en IPv4, el router IPV4-only representa hasta aquí todavía nuestra nube de Internet IPv4 y debe ser transparente para el libre transito de la comunicación entre hosts IPv6.

Esquema de la subred 1 conectada a Internet por medio de un router IPv4-only, un firewall y un Cisco IPv4-only para la salida a Internet, con una dirección IPv4 publica en la interfaz 2 del router 1 (192.0.0.147), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET.

Una vez que probamos la conectividad y funcionamiento de extremo a extremo de las direcciones 6to4 y su encapsulamiento a través de un router IPv4-only y como queremos probar la conectividad hacia el Internet real se implemento el esquema de la Fig. A.12.

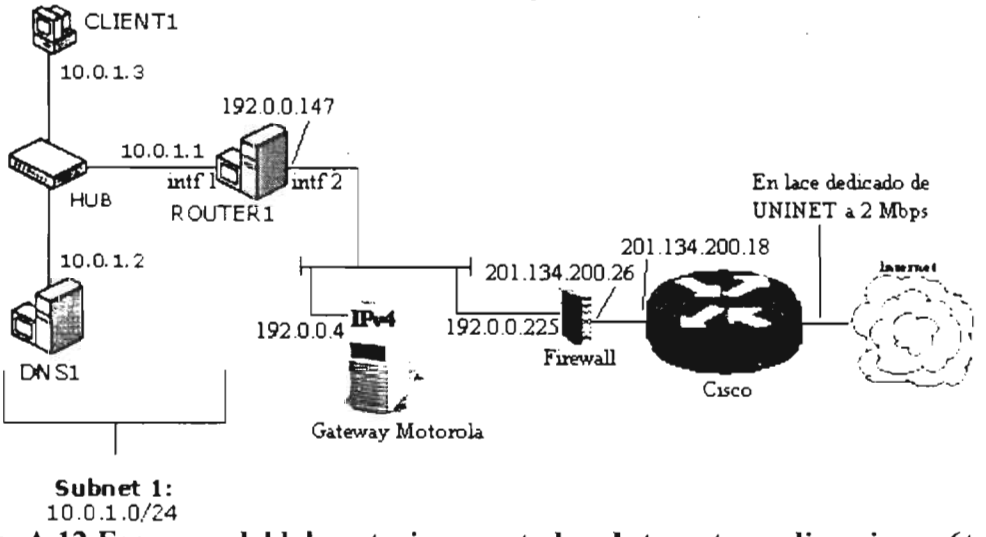


Fig. A.12 Esquema del laboratorio conectado a Internet con direcciones 6to4.

Como se puede ver la subred 1 del laboratorio se conecto a Internet pasando por un router IPv4 only como nuestro gateway, después por un firewall, un cisco IPv4 only y la conexión a Internet por medio de un enlace dedicado de UNINET de 2 Mbps y se hicieron algunas pruebas.
Con este esquema nos pudimos dar cuenta que el firewall no deja pasar el trafico IPv6 encapsulado en IPv4.

Esquema de la subred 1 conectada a Internet por medio de un Cisco IPv4-only de acceso a Internet, con una dirección IPv4 publica homologada en la interfaz 2 del router 1 (201.134.200.25/28), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET.
Por los problemas de conectividad debido al firewall se conecto la subred 1 del laboratorio directamente a Internet IPv4 por medio del enlace dedicado de UNINET de 2 Mbps sin pasar por el firewall, como muestra el esquema de la Fig. A.13

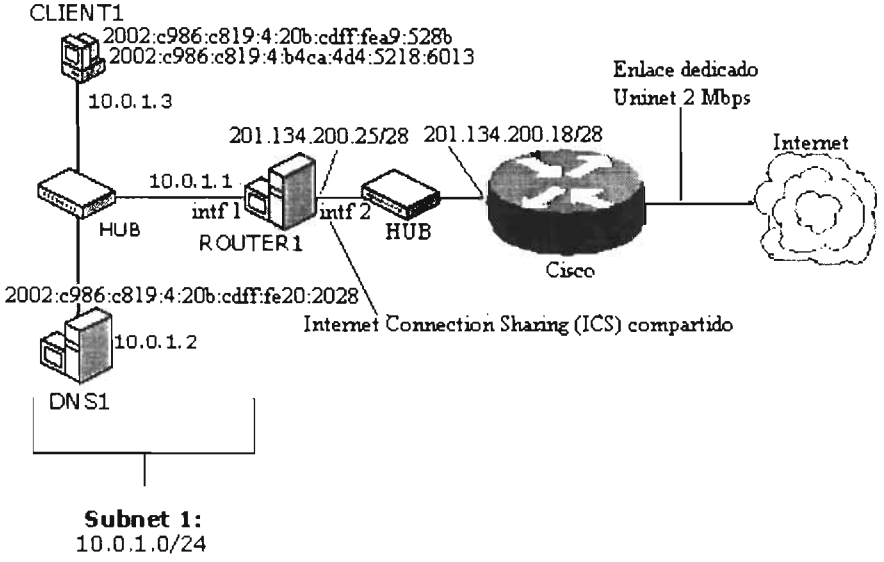


Fig. A.13 Esquema de pruebas con direcciones IPv6 6to4 para la conexión a Internet.

Como se puede observar se tiene una conexión real hacia el Internet IPv4 por medio de un ruteador Cisco que solo maneja IPv4 y ahora en la interfaz 2 del router 1 se configuro una dirección IPv4 publica homologada lo cual nos permite tener conectividad IPv4 hacia Internet, esta dirección provoca que se autoconfiguren direcciones 6to4 y se anuncien sus prefijos a los hosts cliente1 y dns, se realizaron las pruebas correspondientes.
Con este este esquema el router 1 se encarga de encapsular el trafico IPv6 proveniente de la subred 1 para que pueda circular por Internet.

Esquema de la subred 1 y subred 3 conectadas a Internet por medio de un Cisco IPv4-only de acceso a Internet, con una direcciones IPv4 publicas homologadas en las interfaces 2 de los router 1 y 2 (201.134.200.24/28 y 201.134.200.29/28), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET.
Con el esquema anterior solamente tenemos conectividad de los hosts de la subred 1 hacia Internet, y obtenemos respuestas de nuestras peticiones desde las direcciones de Internet pero no podemos checar el otro extremo por lo que se implemento el esquema de la Fig. A.14.

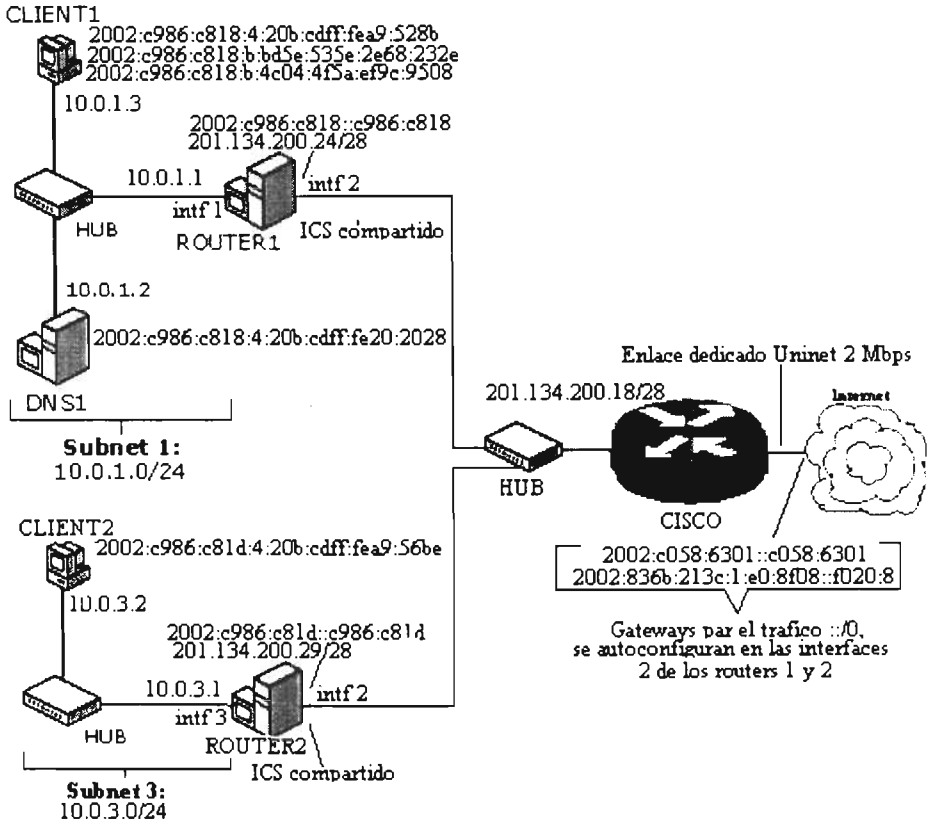


Fig. A.14 Esquema de las subredes 1 y 2 conectadas a Internet con direcciones IPv6 6to4.

Se conecto todo el laboratorio original a Internet IPv4 mediante dos direcciones IPv4 publicas homologadas en los dos routers, así ya podemos hacer pruebas del cliente1 a Internet, del cliente 2 a Internet y del cliente 1 al cliente 2 mediante el uso de direcciones 6to4..

Como podemos observar si probamos con este esquema la conectividad de extremo a extremo de cliente 1 a cliente 2 debido a que tienen direcciones IPv4 publicas homologadas generan direcciones 6to4 que se anuncian a los hosts por tener ICS compartido pero una petición de conexión de cliente1 a cliente2 realmente no viaja por Internet ya que internamente el ruteador cisco sabe que las dos direcciones IPv4 publicas homologadas están en su tarjeta de red Lan por lo que el cisco hará la conexión entre cliente1 y cliente2, es decir un ping de cliente1 a cliente2 no viaja realmente hasta Internet sino que solamente llega hasta el cisco y regresa por su misma interfaz.

Esquema de la subred 1 conectada a Internet por medio de un MODEM DSL de acceso a Internet, con una dirección IPv4 publica dinámica autoconfigurada por DHCP en la interfaz 2 del router 1 (201.128.28.180), con Internet compartido, con un enlace de Prodigy Infinitum de 512 kbps con Telmex. La subred 3 conectada a Internet por medio de un Cisco IPv4-only de acceso a Internet, con una dirección IPv4 publica homologada en la interfaz 2 del router 2 (201.134.200.29/28), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET.

Para tener conectividad entre nuestras dos redes locales IPv6 en forma real como si estuvieran en puntos diferentes los cuales para comunicarse pasan por diferentes accesos a Internet se implemento el esquema de la Fig. A.15:

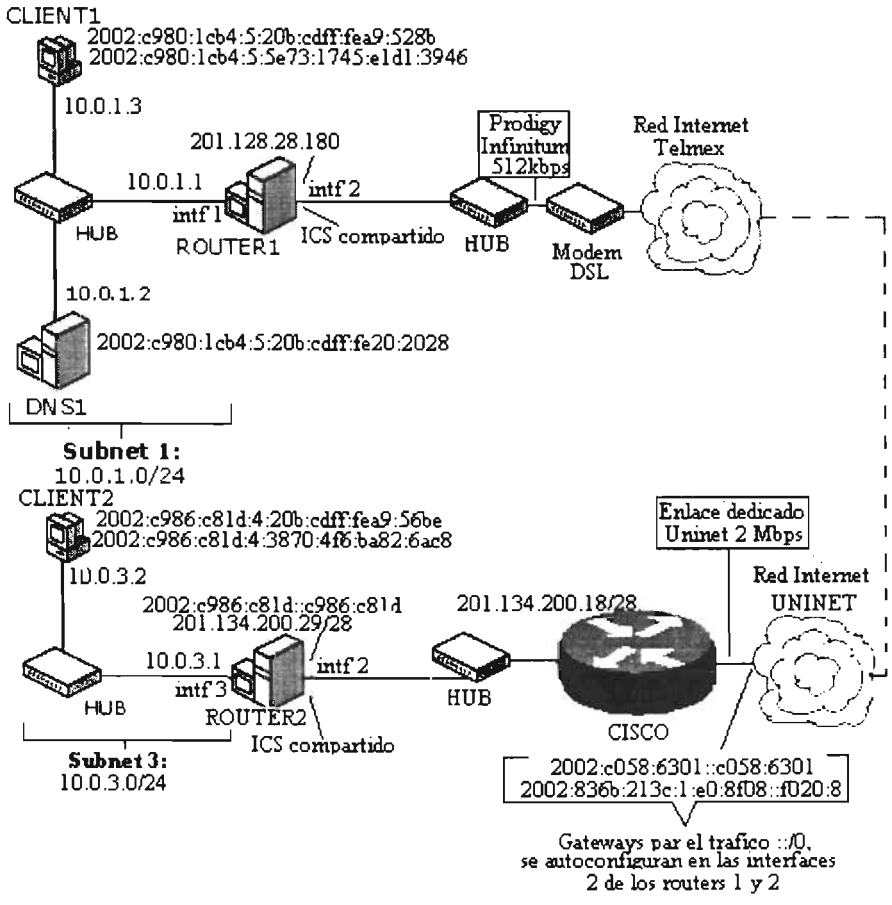


Fig. A.16 Esquema de la subred IPv6 1 conectada a Internet con un enlace DSL y la subred IPv6 2 conectada a Internet con enlace dedicado.

Ahora la subred 1 se conecta a Internet por medio de un enlace contratado con Telmex Infinitum de 512 kbps y la subred 3 se conecta a Internet por medio de un enlace dedicado de 2 Mbps contratado con UNINET con lo cual ahora una petición de ping de cliente 1 a cliente 2 viajara realmente por el Internet IPv4 y probamos en una forma mas real la conectividad extremo a extremo de las direcciones 6to4 pasando por Internet.

Pruebas de seguridad con direcciones IPv6 6to4 globales (2002) que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet, usando además resolución de nombres.

Esquema de la subred 1 y subred 3 conectadas a Internet por medio de un Cisco IPv4-only de acceso a Internet, con una direcciones IPv4 publicas homologadas en las interfaces 2 de los router 1 y 2 (201.134.200.24/28 y 201.134.200.29/28), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET. Con seguridad IPSec ESP desde el cliente1 al router 2 y un túnel AH entre los routers 1 y 2.

Para probar la seguridad con direcciones 6to4 se implemento el esquema de la Fig. A.17:

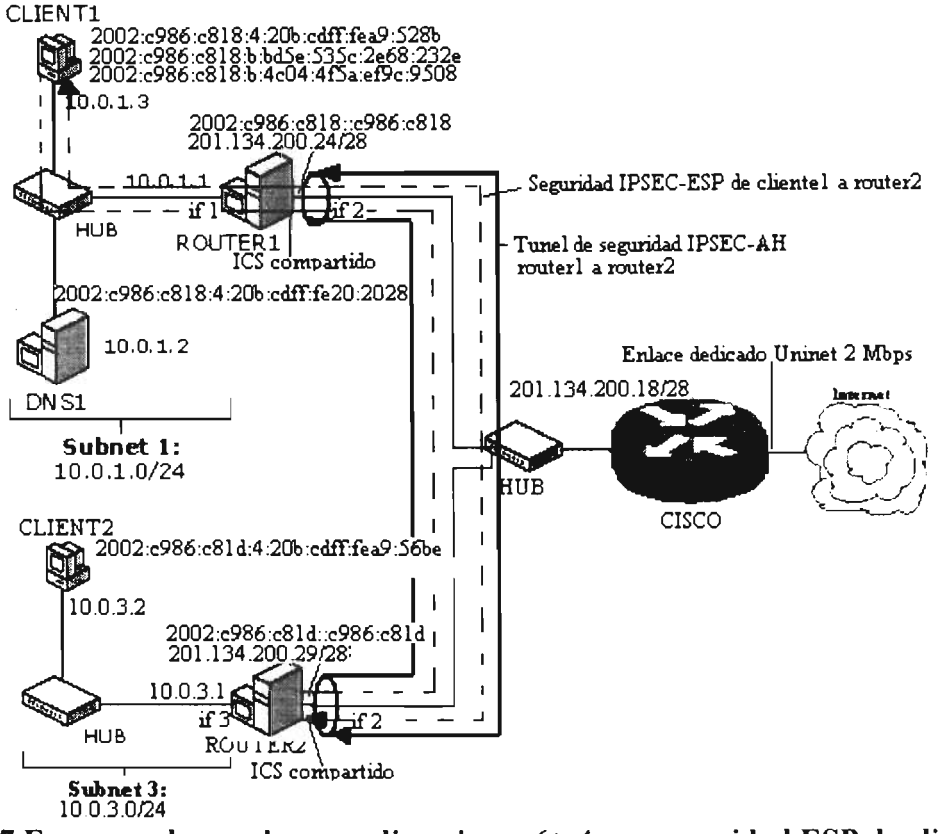


Fig. A.17 Esquema de pruebas con direcciones 6to4 con seguridad ESP de cliente 1 a router2 pasando por un túnel AH.

Esta seguridad vista en forma de bloques es la mostrada en la Fig. A.18:

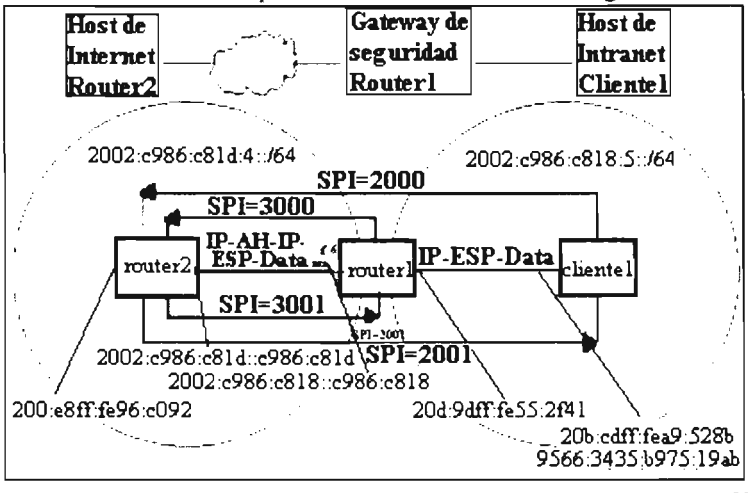


Fig. A.18 Diagrama a bloques de la configuración de seguridad con direcciones 6to4.

Se configuro un túnel de seguridad AH entre los routers 1 y 2 y se configuro la seguridad ESP de cliente 1 a la interfaz 3 del router 2 y se corrieron las pruebas correspondientes.

Pruebas de seguridad con direcciones IPv6 globales (2002) que permiten pasar trafico IPv6 entre nodos que se encuentran en diferentes sitios a través de Internet.

Esquema de la subred 1 y subred 3 conectadas a Internet por medio de un Cisco IPv4-only de acceso a Internet, con una direcciones IPv4 publicas homologadas en las interfaces 2 de los router 1 y 2 (201.134.200.24/28 y 201.134.200.29/28), con Internet compartido, con un enlace de Internet dedicado de 2 Mbps con UNINET. Con seguridad extremo a extremo IPSec ESP desde el cliente1 al cliente 2 y un túnel AH entre los routers 1 y 2.

Por ultimo para probar la conectividad de extremo a extremo con seguridad se empleo el esquema de la Fig. A.19:

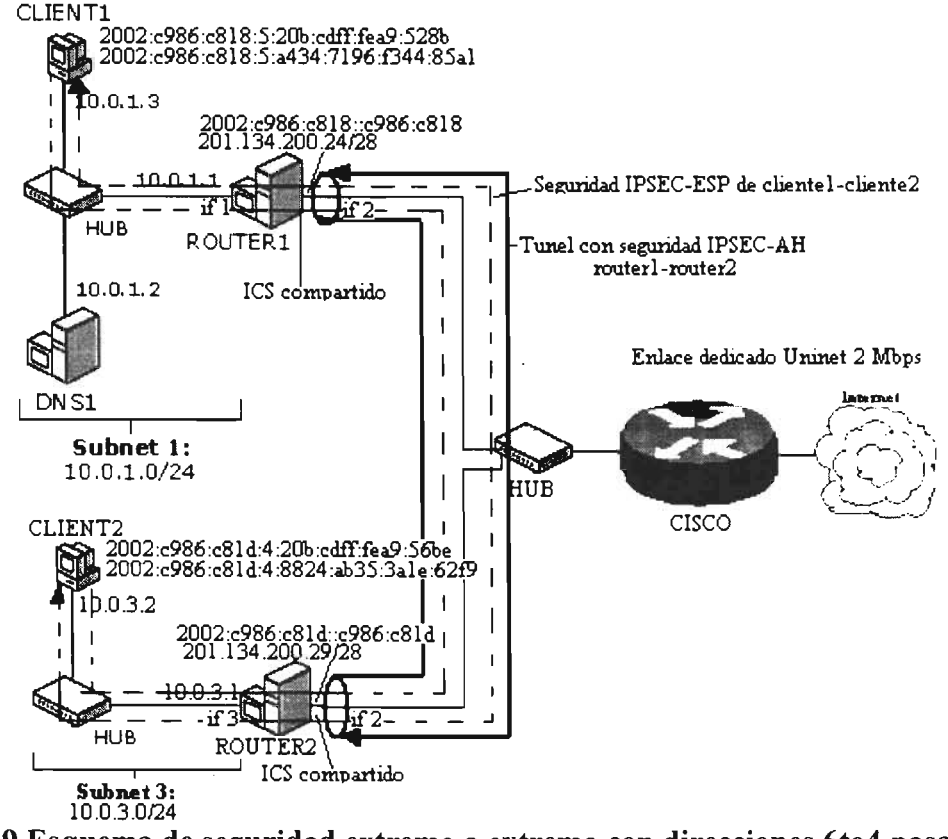


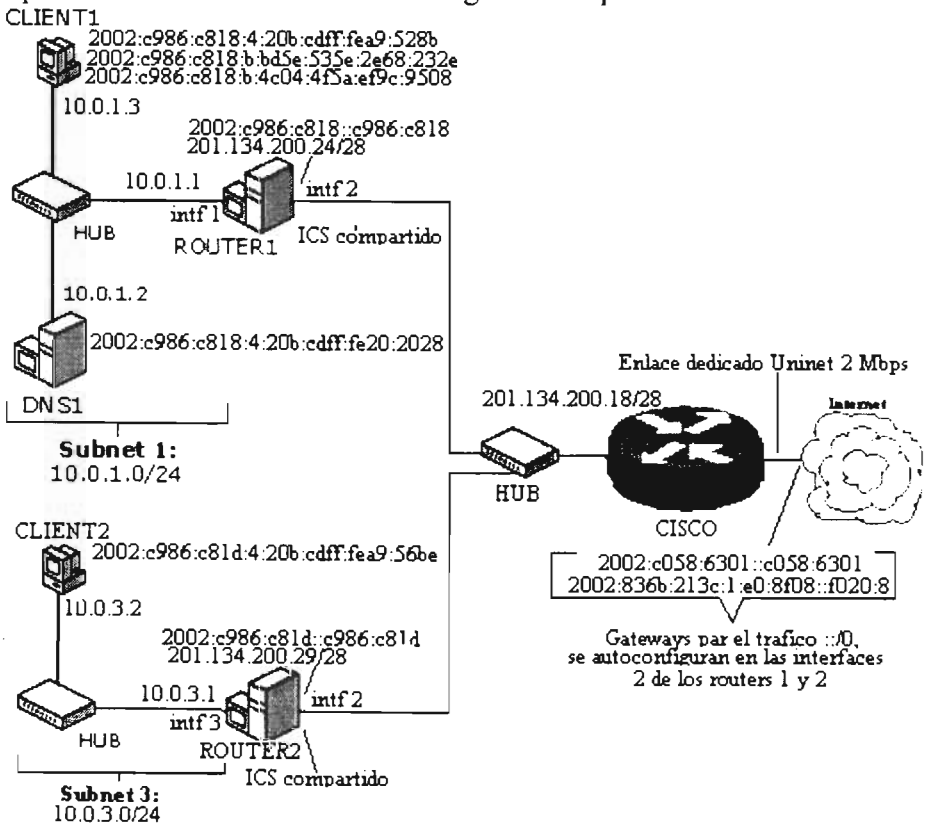
Fig. A.19 Esquema de seguridad extremo a extremo con direcciones 6to4 pasando por un túnel de seguridad AH.

Como se observa se configuro la seguridad ESP de extremo a extremo desde el cliente 1 al cliente 2 pasando por un túnel AH entre los routers 1 y 2.

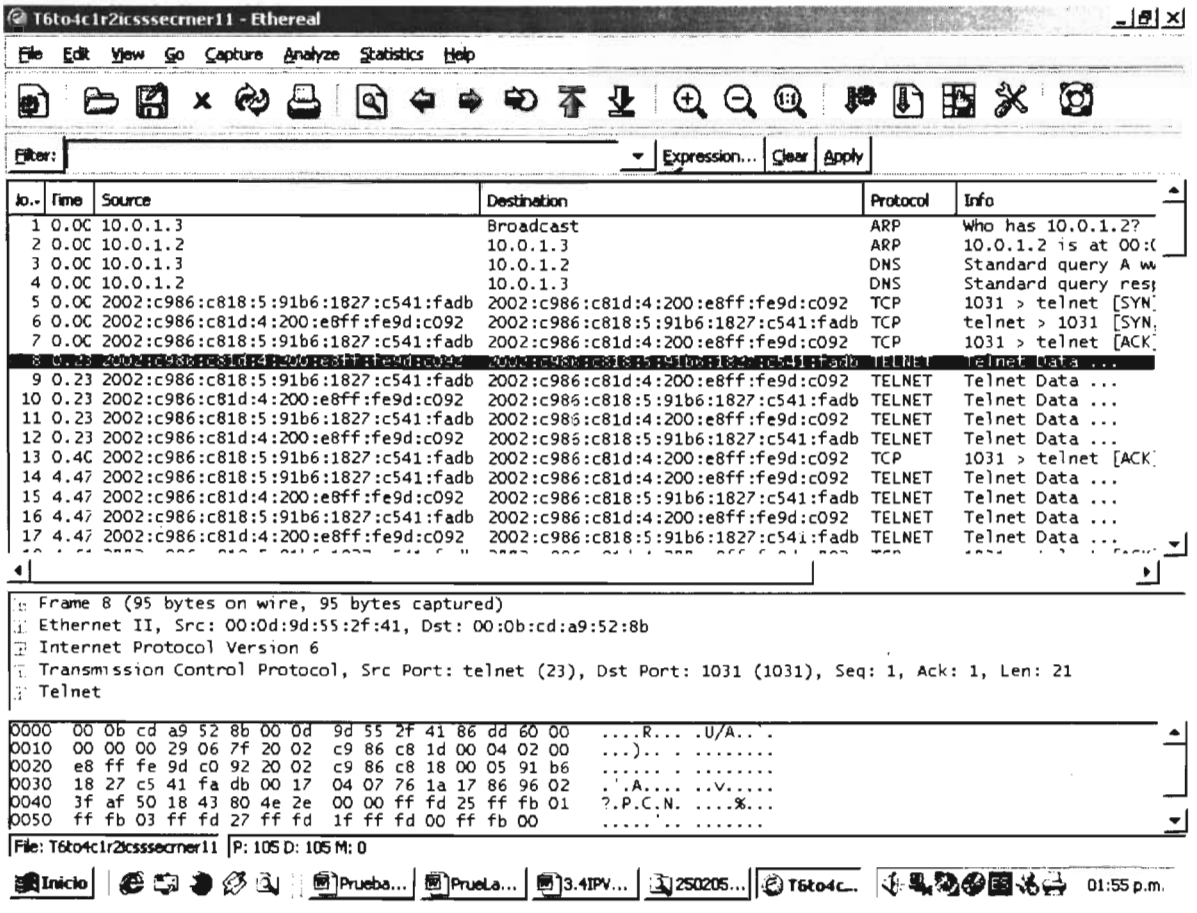
Comparación de la teoría con las pruebas realizadas

- Datagramas eficientes.
  IPv6 busca mejorar la eficiencia en el ruteo mediante el uso de datagramas eficientes y extensibles con un formato de cabecera simplificado en el cual se suprimen algunos campos lo que reduce y simplifica el tratamiento en los ruteadores. Por lo que el paquete de IPv6 tiene 8 campos de encabezado que ocupan 40 bytes y el de IPv4 tiene 12 campos de encabezado que ocupan 20 bytes.

A continuación tenemos un paquete capturado en una conexión con telnet mediante IPv6 y un telnet con IPv4 para comparar los campos que poseen, estos paquetes fueron capturados durante las pruebas fueron realizadas con el siguiente esquema:



Paquete de una conexión telnet con IPv6 capturado en la interfaz 1 del router 1 con ethereal:




```
No.     Time        Source                Destination           Protocol
Info
      8     0.237149                      2002:c986:c81d:4:200:e8ff:fe9d:c092
2002:c986:c818:5:91b6:1827:c541:fadb TELNET   Telnet Data ...

Frame 8 (95 bytes on wire, 95 bytes captured)
    Arrival Time: Feb 25, 2005 09:18:06.851742000
    Time delta from previous packet: 0.232944000 seconds        Preambulo
    Time since reference or first frame: 0.237149000 seconds    de la
    Frame Number: 8                                             trama
    Packet Length: 95 bytes                                     Ethernet
    Capture Length: 95 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 00:0b:cd:a9:52:8b     Encabezado
    Destination: 00:0b:cd:a9:52:8b (10.0.1.3)                   de la
    Source: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)               trama
    Type: IPv6 (0x86dd)                                         Ethernet
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00                                         Encabezado
    Flowlabel: 0x00000                                            del
    Payload length: 41                                          protocolo
    Next header: TCP (0x06)                                       IPv6
    Hop limit: 127
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb
```

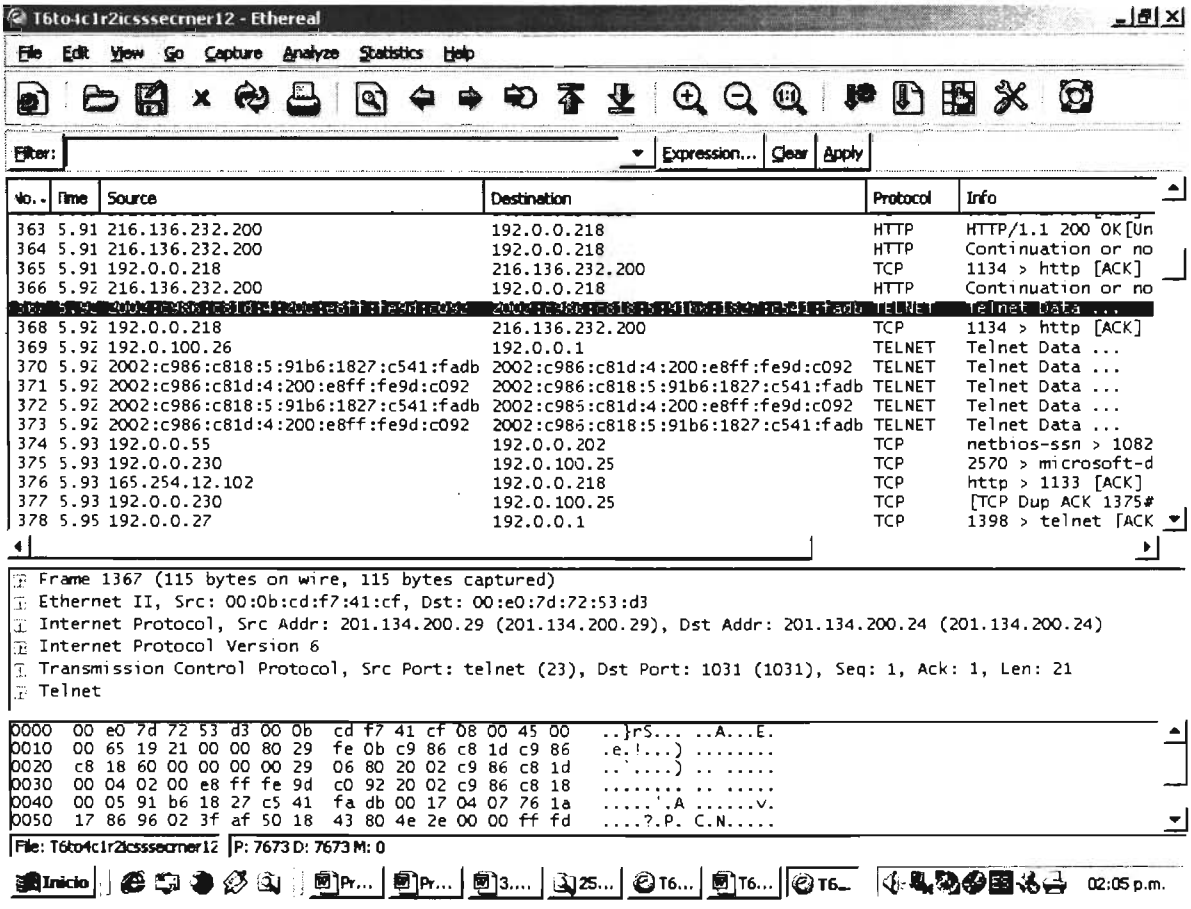
```
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1031
(1031), Seq: 1, Ack: 1, Len: 21
    Source port: telnet (23)
    Destination port: 1031 (1031)
    Sequence number: 1    (relative sequence number)
    Next sequence number: 22    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17280
    Checksum: 0x4e2e (correct)
Telnet
    Command: Do Authentication Option
    Command: Will Echo
    Command: Will Suppress Go Ahead
    Command: Do New Environment Option
    Command: Do Negotiate About Window Size
    Command: Do Binary Transmission
    Command: Will Binary Transmission
```

Encabezado del protocolo de transporte

Datos Aplicación

```
0000  00 0b cd a9 52 8b 00 0d 9d 55 2f 41 86 dd 60 00   ....R....U/A..`.
0010  00 00 00 29 06 7f 20 02 c9 86 c8 1d 00 04 02 00   ...)..  .........
0020  e8 ff fe 9d c0 92 20 02 c9 86 c8 18 00 05 91 b6   ......  .........
0030  18 27 c5 41 fa db 00 17 04 07 76 1a 17 86 96 02   .'.A......v.....
0040  3f af 50 18 43 80 4e 2e 00 00 ff fd 25 ff fb 01   ?.P.C.N.....%...
0050  ff fb 03 ff fd 27 ff fd 1f ff fd 00 ff fb 00      .....'.........
```

Este mismo paquete encapsulado con un encabezado de IPv4 y capturado en la interfaz 2 del router 1 con Ethereal es el siguiente:




```
No.     Time        Source                Destination           Protocol
Info
   1367     5.922525                    2002:c986:c81d:4:200:e8ff:fe9d:c092
2002:c986:c818:5:91b6:1827:c541:fadb TELNET   Telnet Data ...

Frame 1367 (115 bytes on wire, 115 bytes captured)
    Arrival Time: Feb 25, 2005 09:18:06.851704000
    Time delta from previous packet: 0.000116000 seconds
    Time since reference or first frame: 5.922525000 seconds
    Frame Number: 1367
    Packet Length: 115 bytes
    Capture Length: 115 bytes
Ethernet II, Src: 00:0b:cd:f7:41:cf, Dst: 00:e0:7d:72:53:d3
    Destination: 00:e0:7d:72:53:d3 (201.134.200.24)
    Source: 00:0b:cd:f7:41:cf (201.134.200.29)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 201.134.200.29 (201.134.200.29), Dst Addr:
201.134.200.24 (201.134.200.24)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 101
    Identification: 0x1921 (6433)
```

```
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0xfe0b (correct)
    Source: 201.134.200.29 (201.134.200.29)
    Destination: 201.134.200.24 (201.134.200.24)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 41
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1031
(1031), Seq: 1, Ack: 1, Len: 21
    Source port: telnet (23)
    Destination port: 1031 (1031)
    Sequence number: 1    (relative sequence number)
    Next sequence number: 22    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17280
    Checksum: 0x4e2e (correct)
Telnet
    Command: Do Authentication Option
    Command: Will Echo
    Command: Will Suppress Go Ahead
    Command: Do New Environment Option
    Command: Do Negotiate About Window Size
    Command: Do Binary Transmission
    Command: Will Binary Transmission

0000  00 e0 7d 72 53 d3 00 0b cd f7 41 cf 08 00 45 00   ..}rS.....A...E.
0010  00 65 19 21 00 00 80 29 fe 0b c9 86 c8 1d c9 86   .e.!...).........
0020  c8 18 60 00 00 00 00 29 06 80 20 02 c9 86 c8 1d   ..`....).. ......
0030  00 04 02 00 e8 ff fe 9d c0 92 20 02 c9 86 c8 18   .......... ......
0040  00 05 91 b6 18 27 c5 41 fa db 00 17 04 07 76 1a   .....'.A......v.
0050  17 86 96 02 3f af 50 18 43 80 4e 2e 00 00 ff fd   ....?.P.C.N.....
0060  25 ff fb 01 ff fb 03 ff fd 27 ff fd 1f ff fd 00   %........'......
0070  ff fb 00                                          ...
```

Para compararlos tenemos a continuación la parte del encabezado de IPv6 del primer paquete capturado:

Campo del paquete IPv6	Longitud en bytes=40 bytes
Version: 6	4 bytes
Traffic class: 0x00	
Flowlabel: 0x00000	
Payload length: 41	2 bytes
Next header: TCP (0x06)	1 byte
Hop limit: 127	1 byte
Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092	16 bytes
Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb	16 bytes

La parte del encabezado de IPv4 del segundo paquete capturado es:

Campo del paquete IPv4	Longitud en bytes=20 bytes
Version: 4	1 byte
Header length: 20 bytes	1 byte
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..0. = ECN-Capable Transport (ECT): 0 ....0 = ECN-CE: 0	1 byte
Total Length: 101	2 bytes
Identification: 0x1921 (6433)	2 bytes
Flags: 0x00 0... = Reserved bit: Not set .0.. = Don't fragment: Not set ..0. = More fragments: Not set	1 byte
Fragment offset: 0	2 bytes
Time to live: 128	1 byte
Protocol: IPv6 (0x29)	1 byte
Header checksum: 0xfe0b (correct)	2 bytes
Source: 201.134.200.29	4 bytes
Destination: 201.134.200.24	4 bytes

Podemos ver que el encabezado de IPv6 es de 40 bytes y el de IPv4 es de 20 bytes.
Comparando los encabezados de IPv6 e IPv4 se puede ver claramente la diferencia de campos, el encabezado de IPv6 tiene menos campos que el encabezado de IPv4, como el paquete de IPv6 tiene menos campos permitirá que los ruteadores consuman menos tiempo en el procesamiento de cada paquete puesto que tendrán menos campos que revisar. El encabezado de IPv4 tiene al menos 12 campos y el de IPv6 tiene 8 campos, el procesar un mayor numero de campos requerirá mas memoria y tiempo de procesamiento en los ruteadores, puesto que además de tener que revisar mas campos algunos de ellos tienen que ser revisados bit por bit como son los campos de servicios diferenciados o el de banderas,

en estos campos el ruteador tiene que revisar bit por bit ya que cada uno de ellos representa algún valor o acción que el ruteador tiene que realizar, por ejemplo alguno de los bits de los campos de IPv4 pueden indicar si el paquete esta fragmentado, si hay mas fragmentos, etc., por lo que el ruteador tardara mas tiempo en procesar el paquete.

- Los paquetes IPv6 son transportados sobre Ethernet con el contenido tipo (content type) 86DD en hexadecimal, en lugar del 0800 de IPv4

Esto se cumple ya que en cualquiera de los paquetes capturados para IPv4, el encabezado de Ethernet maneja en tipo 0800 y para IPv6 maneja 86DD:

Extracto de un paquete IPv4 con el encabezado Ethernet para IPV4:

```
Ethernet II, Src: 00:0b:cd:f7:41:cf, Dst: 00:e0:7d:72:53:d3
    Destination: 00:e0:7d:72:53:d3 (201.134.200.24)
    Source: 00:0b:cd:f7:41:cf (201.134.200.29)
    Type: IP (0x0800)
```

Extracto de un paquete IPv6 con el encabezado Ethernet para IPV6:

```
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 00:0b:cd:a9:52:8b
    Destination: 00:0b:cd:a9:52:8b (10.0.1.3)
    Source: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)
    Type: IPv6 (0x86dd)
```

- Comprobación de errores.
  En IPv6 se elimina el control de errores en la cabecera.

Esto se comprueba ya que podemos ver en los dos paquetes capturados que en el paquete de IPv6 se ha eliminado el control de errores en la cabecera ya que no presenta el campo checksum. El paquete de IPv4 si comprueba errores con la comprobación de suma (checksum). IPv6 deja estas comprobaciones a los niveles superiores.

Extracto de un paquete IPv4, este posee comprobación de errores:

```
Internet Protocol, Src Addr: 201.134.200.29 (201.134.200.29), Dst Addr:
201.134.200.24 (201.134.200.24)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 101
    Identification: 0x1921 (6433)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0xfe0b (correct)
    Source: 201.134.200.29 (201.134.200.29)
    Destination: 201.134.200.24 (201.134.200.24)
```

Extracto de un paquete IPv6, este no posee comprobación de errores:

```
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 41
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb
```

- Fragmentación.
  IPv6 realiza la fragmentación solo en la fuente ya que los paquetes IP son eficientes y extensibles sin que haya necesidad de realizar la fragmentación en los routers pues son alineados a 64 bits con su cabecera de longitud fija más simple que agiliza su procesado por parte del router.

Podemos observar en los paquetes capturados que la cabecera de IPv6 ya no posee bits de fragmentación como si los tiene la de IPv4, este campo fue removido del encabezado.

Extracto de un paquete IPv4, este posee bits de fragmentación:

```
Internet Protocol, Src Addr: 201.134.200.29 (201.134.200.29), Dst Addr:
201.134.200.24 (201.134.200.24)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 101
    Identification: 0x1921 (6433)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0xfe0b (correct)
    Source: 201.134.200.29 (201.134.200.29)
    Destination: 201.134.200.24 (201.134.200.24)
```

Extracto de un paquete IPv6, este no posee comprobación de errores:

```
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 41
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb
```

- Calidad de servicio.
  También en la teoría hablamos de la característica de IPv6 calidad de servicio que permite administrar flujos de datagramas pertenecientes a servicios especiales mediante el manejo de etiquetas de flujo. Permite realizar una asignación más fácil de recursos pues permite el etiquetado de los paquetes como pertenecientes a un flujo de trafico particular para el cual el emisor solicita un tratamiento especial, lo que ayuda a tratar con trafico especializado como el video, audio o la voz en tiempo real..

En los paquetes capturados podemos ver como se tiene un campo de 4 bytes llamado FlowLabel usado para este fin junto con el campo traffic class.

Extracto de un paquete IPv4, este intenta proporcionar calidad de servicio únicamente con el campo servicios diferenciados:

```
Internet Protocol, Src Addr: 201.134.200.29 (201.134.200.29), Dst Addr:
201.134.200.24 (201.134.200.24)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 101
    Identification: 0x1921 (6433)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0xfe0b (correct)
    Source: 201.134.200.29 (201.134.200.29)
    Destination: 201.134.200.24 (201.134.200.24)
```

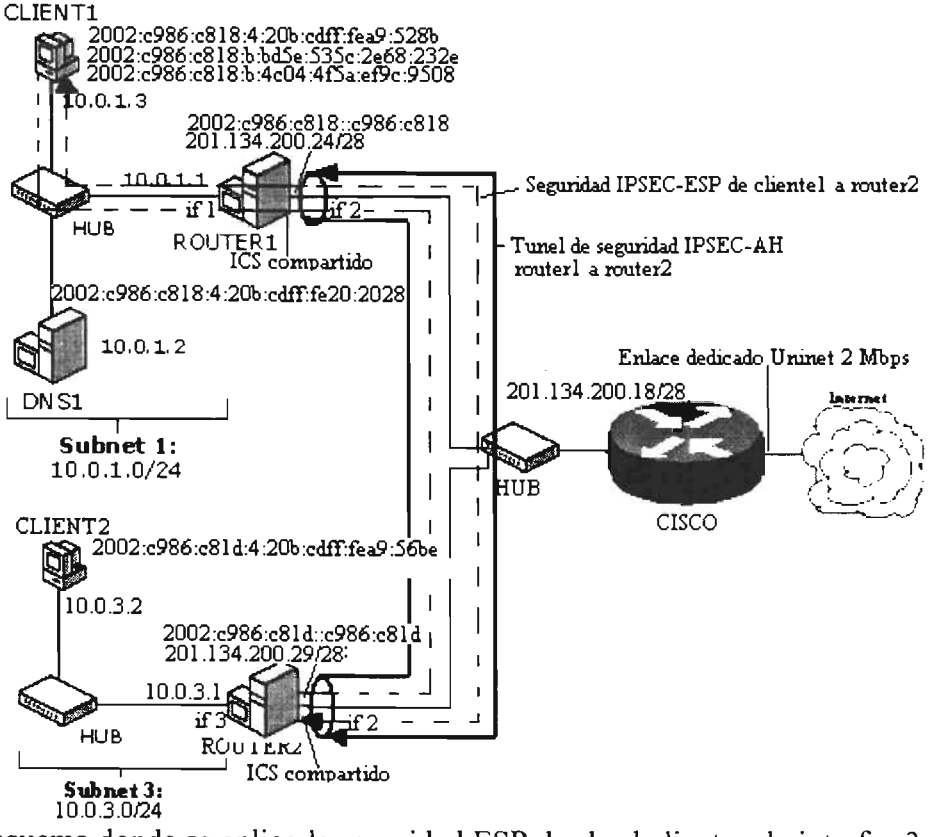
Extracto de un paquete IPv6, este proporciona calidad de servicio con el campo etiqueta de flujo y clase de trafico:

```
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 41
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:91b6:1827:c541:fadb
```

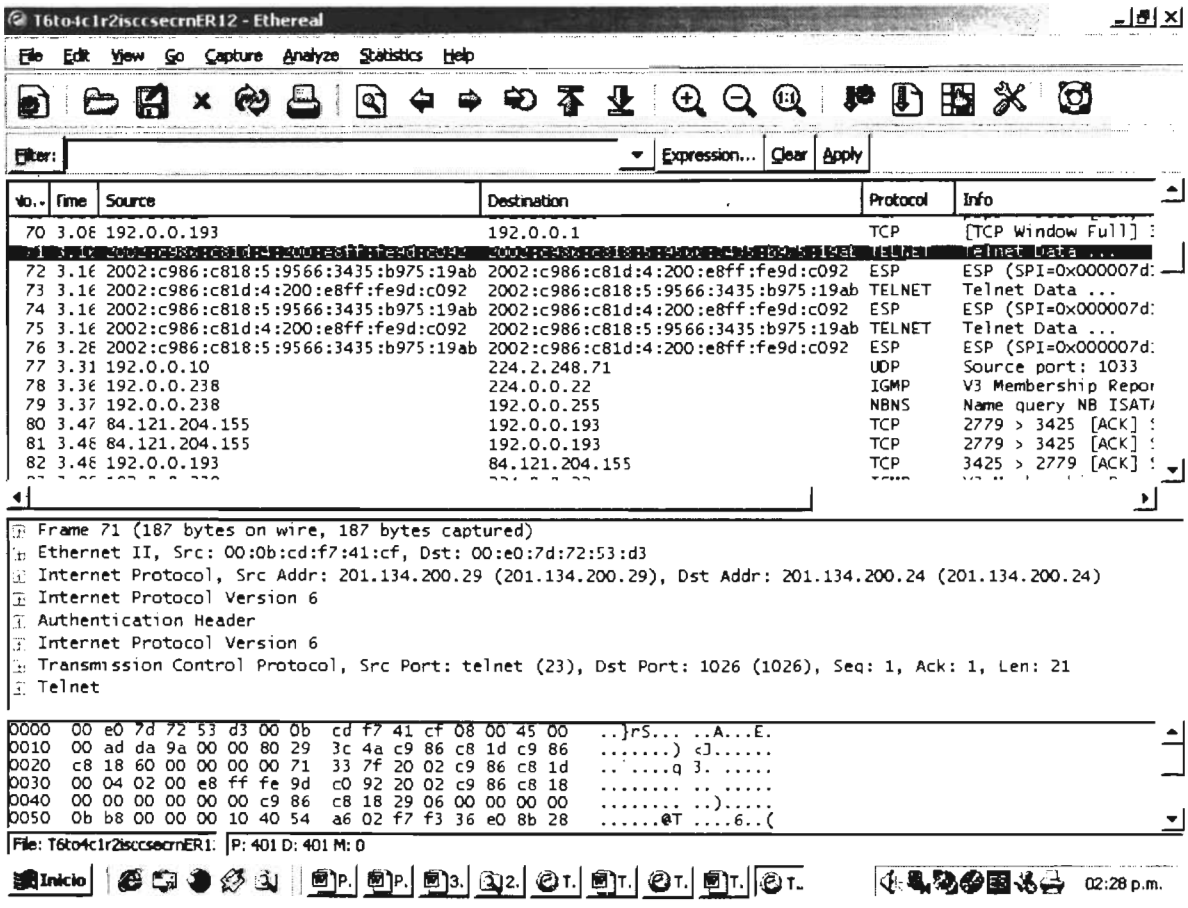
- Cabeceras de extensión.
  Posibilidades de extensión de las cabeceras y de las opciones. En IPv6 las opciones están contenidas en cabeceras suplementarias colocadas entre la cabecera IPv6 y la cabecera del paquete de transporte (T-PDU Transport Protocol Data Unit). La mayoría de las opciones de las cabeceras de IPv6 no son examinadas ni tratadas por los ruteadores intermedios. Esto simplifica y acelera el procesamiento que realiza un

dispositivo de ruteo sobre los datagramas IPv6 en comparación a los datagramas IPv4 a la vez que es más fácil incorporar opciones adicionales.

Pudimos comprobar que las cabeceras opcionales en IPv6 son introducidas entre la cabecera principal y la de transporte, por ejemplo si aplicamos seguridad AH a un paquete la cabecera indicando este tipo de seguridad se introduce entre la cabecera principal de IPv6 y la de transporte, se uso tomo un paquete de las pruebas realizadas con el siguiente esquema:



En este esquema donde se aplico la seguridad ESP desde el cliente a la interfaz 3 del router 2 pasando por un tunel AH entre los router 1 y 2 se capturo el siguiente paquete con ethereal:




```
No.      Time         Source                Destination           Protocol
Info
     71     3.160827                    2002:c986:c81d:4:200:e8ff:fe9d:c092
2002:c986:c818:5:9566:3435:b975:19ab TELNET   Telnet Data ...

Frame 71 (187 bytes on wire, 187 bytes captured)
    Arrival Time: Feb 25, 2005 16:46:40.714868000
    Time delta from previous packet: 0.233564000 seconds
    Time since reference or first frame: 3.160827000 seconds
    Frame Number: 71
    Packet Length: 187 bytes
    Capture Length: 187 bytes
Ethernet II, Src: 00:0b:cd:f7:41:cf, Dst: 00:e0:7d:72:53:d3
    Destination: 00:e0:7d:72:53:d3 (201.134.200.24)
    Source: 00:0b:cd:f7:41:cf (201.134.200.29)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 201.134.200.29 (201.134.200.29), Dst Addr:
201.134.200.24 (201.134.200.24)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 173
    Identification: 0xda9a (55962)
```

```
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0x3c4a (correct)
    Source: 201.134.200.29 (201.134.200.29)
    Destination: 201.134.200.24 (201.134.200.24)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 113
    Next header: AH (0x33)
    Hop limit: 127
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818::c986:c818
Authentication Header
    Next Header: IPv6 (0x29)
    Length: 32
    SPI: 0x00000bb8
    Sequence: 16
    ICV
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 41
    Next header: TCP (0x06)
    Hop limit: 128
    Source address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
    Destination address: 2002:c986:c818:5:9566:3435:b975:19ab
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1026
(1026), Seq: 1, Ack: 1, Len: 21
    Source port: telnet (23)
    Destination port: 1026 (1026)
    Sequence number: 1    (relative sequence number)
    Next sequence number: 22    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17280
    Checksum: 0xb223 (correct)
Telnet
    Command: Do Authentication Option
    Command: Will Echo
    Command: Will Suppress Go Ahead
```

Cabecera de extensión la cabecera IPv6 y el encabezado transporte

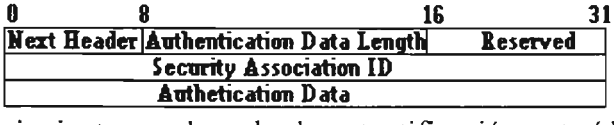
```
Command: Do New Environment Option
Command: Do Negotiate About Window Size
Command: Do Binary Transmission
Command: Will Binary Transmission
```

Podemos comprobar como la cabecera opcional de autentificación del encabezado es insertada después del encabezado IPV6.
En el paquete capturado podemos ver como la seguridad se ha puesto como un encabezado entre el de IPv6 y el de transporte, además la teoría nos dice que el encabezado de autentificación será indicado en el campo next header=51 lo cual si se comprueba en nuestro paquete capturado ya que el campo del encabezado de IPv6 indica next header=33 este valor esta en hexadecimal que convertido a decimal 33=00110011=51 lo cual coincide con la teoría. La teoría dice que este encabezado adicional al de IPv6 no será examinado por los routers intermedios solamente por el destino y más en este caso que se trata de una cabecera opcional de seguridad con una llave configurada que solamente el destino posee la llave para desencapsular la autentificación y por lo tanto solamente el destino será el que examine este encabezado.

- IPv6 Proporciona capacidades de seguridad mediante el uso de las posibilidades de autentificación y confidencialidad. IPv6 define extensiones que permiten la autentificación de los usuarios y la integridad de los datos mediante herramientas de criptografía. El soporte de IPsec es un requerimiento del protocolo IPv6 para tener seguridad desde el núcleo del protocolo.

Con las pruebas realizadas pudimos comprobar que la seguridad de autentificación y confidencialidad (AH y ESP) funcionan perfectamente.

- Cabecera de autentificación
  Esta cabecera autentifica y asegura la integridad de los paquetes. En el campo Next Header del encabezado principal su valor es de 51, sus campos se observan en la siguiente figura:



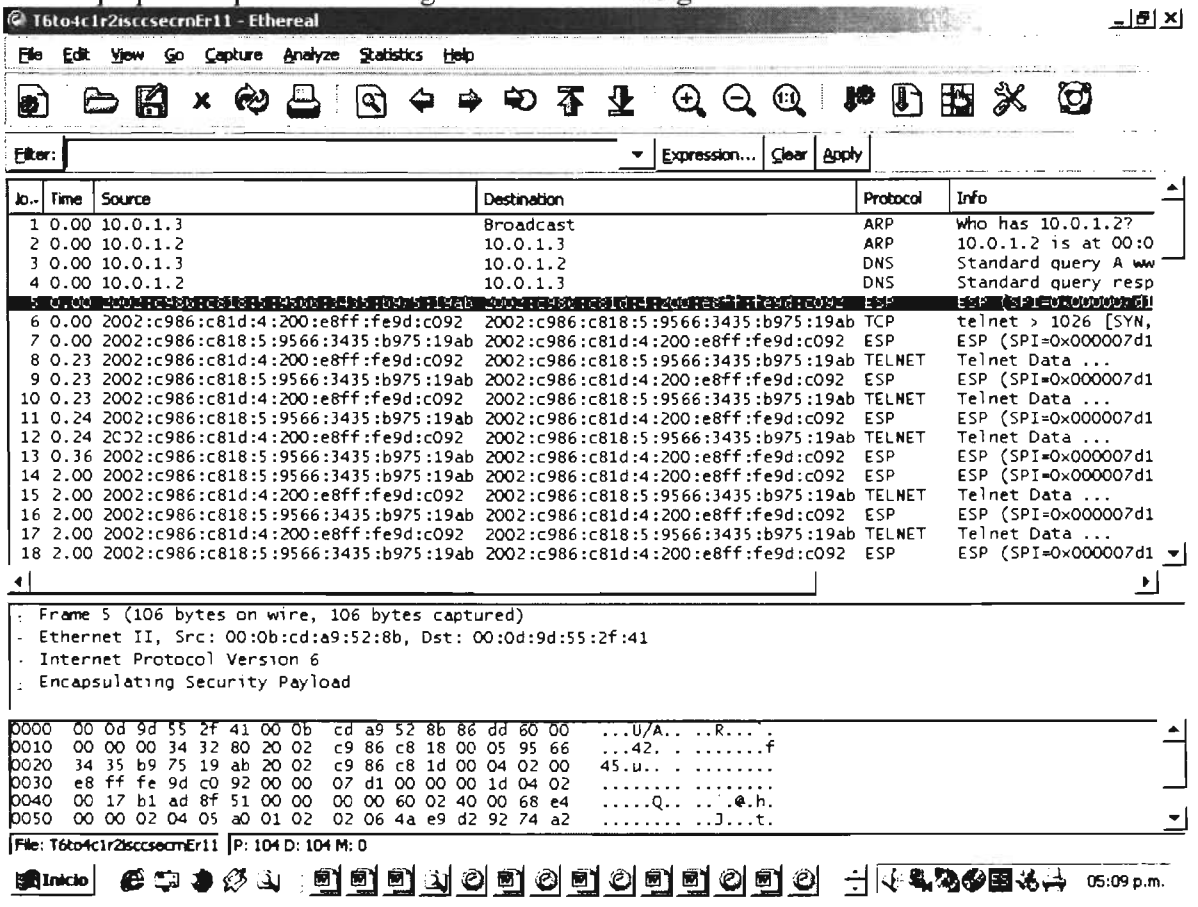
Esto se cumple en el siguiente encabezado de autentificación extraído de la captura de un paquete capturado:

```
Authentication Header
    Next Header: IPv6 (0x29)
    Length: 32
    SPI: 0x00000bb8
    Sequence: 16
    ICV
```

- Cabecera de confidencialidad
  Evita el acceso no autorizado al paquete, encriptando los datos y colocándolos en la parte correspondiente de la cabecera de confidencialidad. Se puede solamente encriptar la trama del nivel de transporte o el datagrama entero. Esta cabecera es siempre el ultimo campo no encriptado de un paquete. Funciona entre estaciones, entre una estación y un firewall o entre firewalls. Los campos de esta cabecera son:

Security Association Identifier		
Initialization Vector		
Next Header	Length	Reserved
Protected Data		
Trailer		

Así un paquete capturado con seguridad ESP es el siguiente:




```
No.     Time        Source                Destination           Protocol
Info
       5     0.002218                    2002:c986:c818:5:9566:3435:b975:19ab
2002:c986:c81d:4:200:e8ff:fe9d:c092 ESP      ESP (SPI=0x000007d1)

Frame 5 (106 bytes on wire, 106 bytes captured)
    Arrival Time: Feb 25, 2005 16:46:40.479328000
    Time delta from previous packet: 0.001258000 seconds
    Time since reference or first frame: 0.002218000 seconds
    Frame Number: 5
    Packet Length: 106 bytes
    Capture Length: 106 bytes
Ethernet II, Src: 00:0b:cd:a9:52:8b, Dst: 00:0d:9d:55:2f:41
    Destination: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)
    Source: 00:0b:cd:a9:52:8b (10.0.1.3)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
```

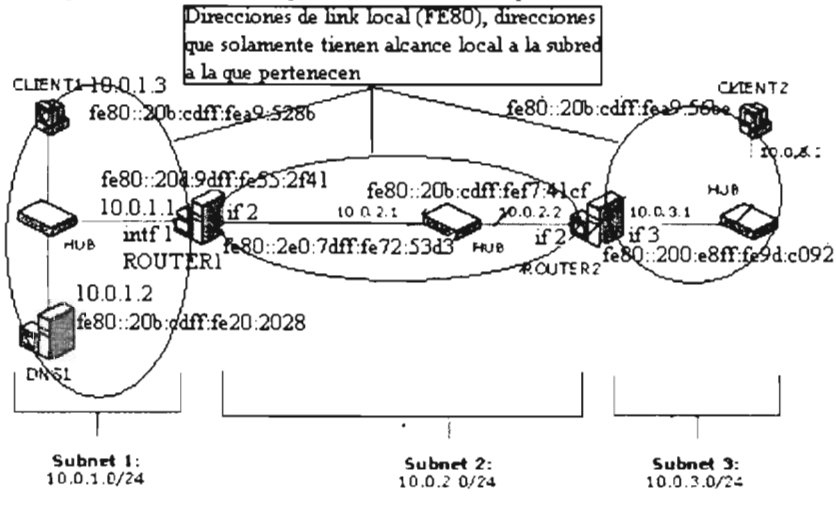
```
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 52
    Next header: ESP (0x32)
    Hop limit: 128
    Source address: 2002:c986:c818:5:9566:3435:b975:19ab
    Destination address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
Encapsulating Security Payload
    SPI: 0x000007d1
    Sequence: 29
    Data (44 bytes)

0000  00 0d 9d 55 2f 41 00 0b cd a9 52 8b 86 dd 60 00   ...U/A....R...`.
0010  00 00 00 34 32 80 20 02 c9 86 c8 18 00 05 95 66   ...42. ........f
0020  34 35 b9 75 19 ab 20 02 c9 86 c8 1d 00 04 02 00   45.u.. ........
0030  e8 ff fe 9d c0 92 00 00 07 d1 00 00 00 1d 04 02   ................
0040  00 17 b1 ad 8f 51 00 00 00 00 60 02 40 00 68 e4   .....Q....`.@.h.
0050  00 00 02 04 05 a0 01 02 02 06 4a e9 d2 92 74 a2   ..........J...t.
0060  ca 35 89 cd 52 f9 b5 2f 40 4c                     .5..R../@L
```

Podemos ver que se cumple la teoría ya que encapsula la cabecera de transporte y vemos que es el ultimo encabezado del paquete y cumple con los campos mencionados del encabezado.

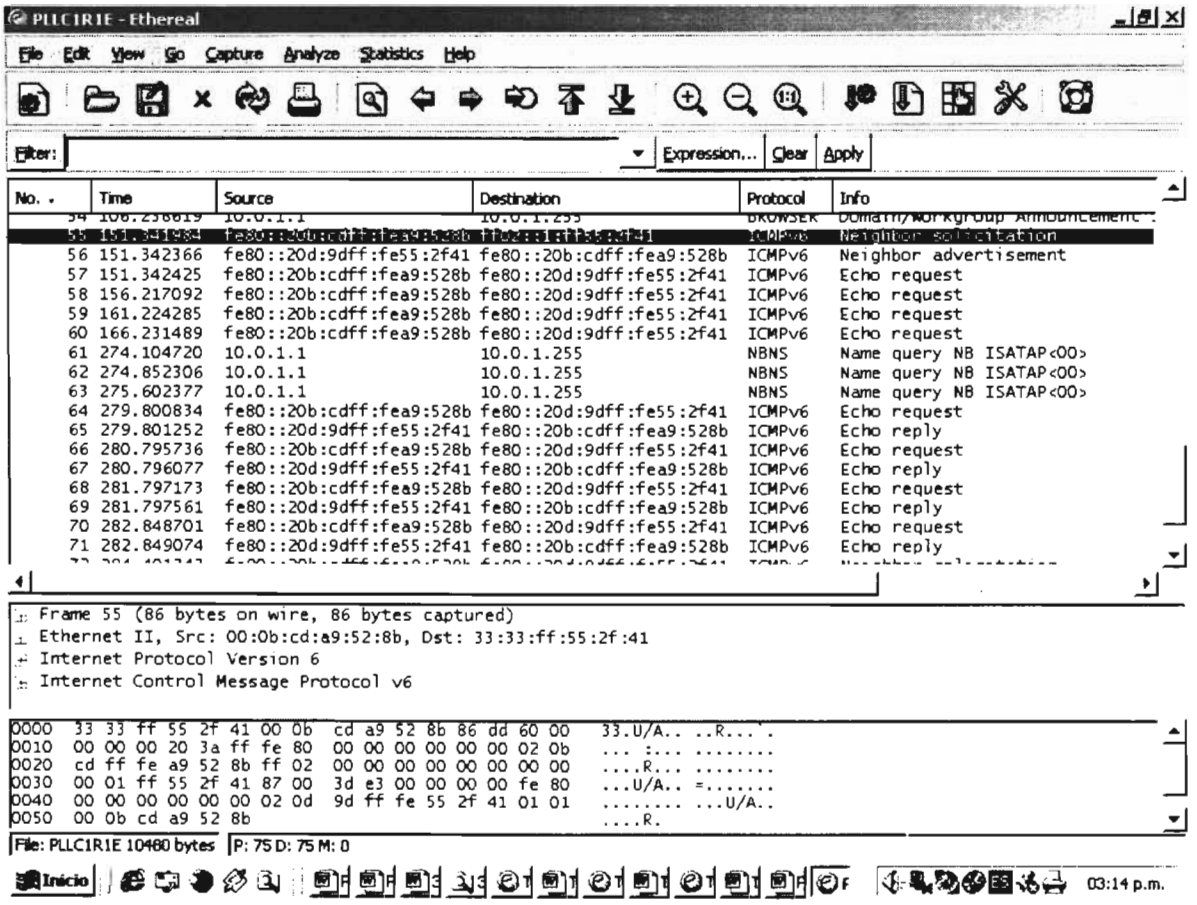
- Mayor flexibilidad de direccionamiento ya que incluye el concepto de dirección de monodistribución o envío a uno (anycast), este concepto permite entregar un paquete solamente a un nodo seleccionado entre un conjunto de nodos.

Para verificar esto podemos visualizar el dialogo que realizan los equipos de solicitud de vecino (neighbor solicitation) y anunciamiento de router, estos diálogos es una característica de IPv6 ya que mediante ellos es como los hosts escuchan el y captan el prefijo para autoconfigurar la dirección IPv6, como se puede observar en la siguiente captura con direcciones link local:

Este paquete se capturo durante las pruebas con el esquema de direcciones de link local:



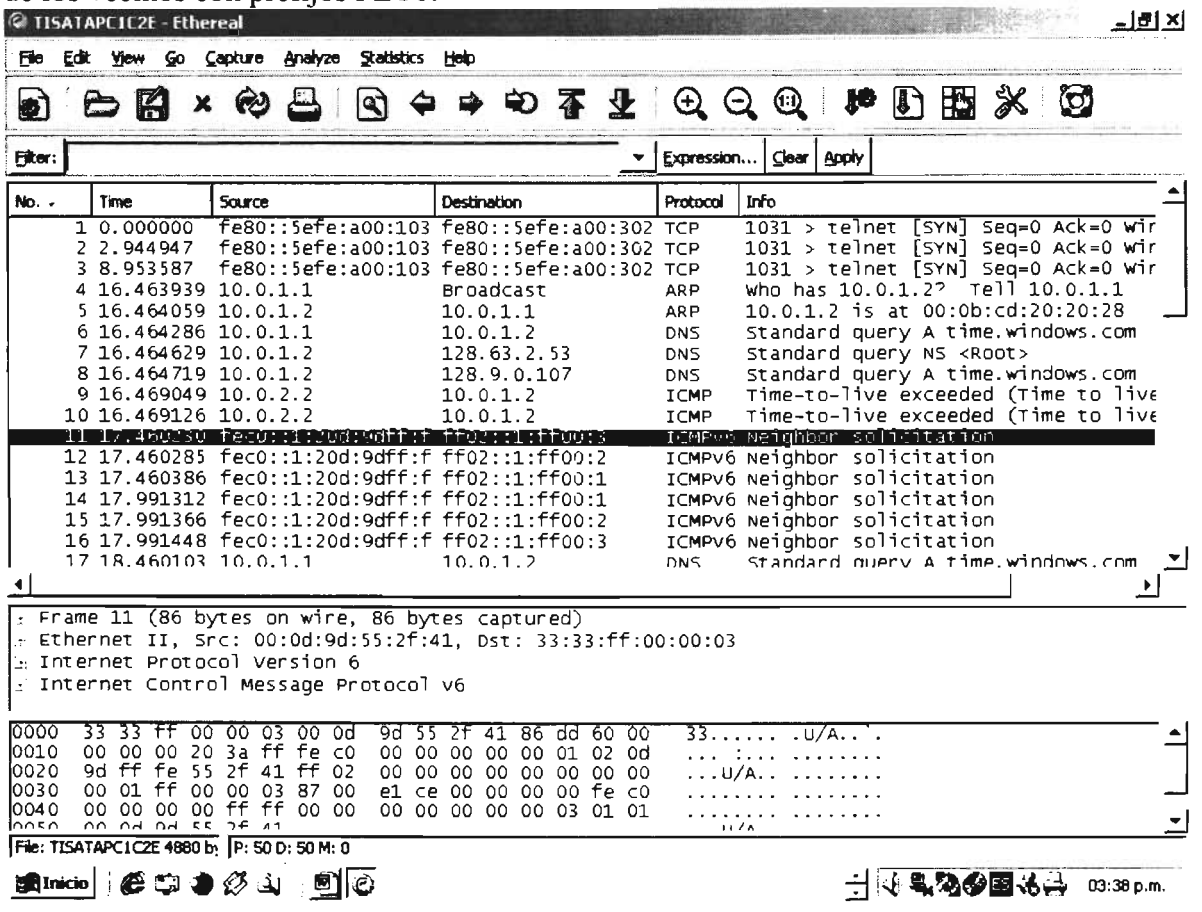
Captura de un paquete de solicitud de vecinos en el cliente 1:




```
No.     Time        Source                Destination           Protocol
Info
     55 151.341984  fe80::20b:cdff:fea9:528b ff02::1:ff55:2f41      ICMPv6
Neighbor solicitation

Frame 55 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Jan 31, 2005 11:12:31.305203000
    Time delta from previous packet: 45.103365000 seconds
    Time since reference or first frame: 151.341984000 seconds
    Frame Number: 55
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0b:cd:a9:52:8b, Dst: 33:33:ff:55:2f:41
    Destination: 33:33:ff:55:2f:41 (IPv6-Neighbor-Discovery_ff:55:2f:41)
    Source: 00:0b:cd:a9:52:8b (10.0.1.3)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::20b:cdff:fea9:528b        Busqueda de un
    Destination address: ff02::1:ff55:2f41      conjunto de nodos
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
```

```
    Code: 0
    Checksum: 0x3de3 (correct)                    Busqueda de un
    Target: fe80::20d:9dff:fe55:2f41              solo nodo
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0b:cd:a9:52:8b

0000  33 33 ff 55 2f 41 00 0b cd a9 52 8b 86 dd 60 00   33.U/A....R...`.
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 02 0b   ... :...........
0020  cd ff fe a9 52 8b ff 02 00 00 00 00 00 00 00 00   ....R...........
0030  00 01 ff 55 2f 41 87 00 3d e3 00 00 00 00 fe 80   ...U/A..=.......
0040  00 00 00 00 00 00 02 0d 9d ff fe 55 2f 41 01 01   ...........U/A..
0050  00 0b cd a9 52 8b                                 ....R.

No.     Time        Source                Destination           Protocol
Info
     56  151.342366     fe80::20d:9dff:fe55:2f41  fe80::20b:cdff:fea9:528b
ICMPv6   Neighbor advertisement

Frame 56 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Jan 31, 2005 11:12:31.305585000
    Time delta from previous packet: 0.000382000 seconds
    Time since reference or first frame: 151.342366000 seconds
    Frame Number: 56
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 00:0b:cd:a9:52:8b
    Destination: 00:0b:cd:a9:52:8b (10.0.1.3)
    Source: 00:0d:9d:55:2f:41 (10.0.1.1)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::20d:9dff:fe55:2f41
    Destination address: fe80::20b:cdff:fea9:528b
Internet Control Message Protocol v6
    Type: 136 (Neighbor advertisement)
    Code: 0
    Checksum: 0x90f5 (correct)
    Flags: 0x60000000
        0... .... .... .... .... .... .... .... = Not router
        .1.. .... .... .... .... .... .... .... = Solicited
        ..1. .... .... .... .... .... .... .... = Override
    Target: fe80::20d:9dff:fe55:2f41
    ICMPv6 options
        Type: 2 (Target link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41
```

También en los siguientes 3 paquetes tenemos como un nodo hace peticiones en búsqueda de los vecinos con prefijos FEC0:




```
No.     Time        Source                Destination           Protocol
Info
    11  17.460230   fec0::1:20d:9dff:fe55:2f41  ff02::1:ff00:3
ICMPv6  Neighbor solicitation

Frame 11 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Feb  7, 2005 20:51:09.529246000
    Time delta from previous packet: 0.991104000 seconds
    Time since reference or first frame: 17.460230000 seconds
    Frame Number: 11
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 33:33:ff:00:00:03
    Destination: 33:33:ff:00:00:03 (IPv6-Neighbor-Discovery_ff:00:00:03)
    Source: 00:0d:9d:55:2f:41 (10.0.1.1)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fec0::1:20d:9dff:fe55:2f41
```

```
    Destination address: ff02::1:ff00:3
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0xe1ce (correct)
    Target: fec0:0:0:ffff::3
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41

0000  33 33 ff 00 00 03 00 0d 9d 55 2f 41 86 dd 60 00   33.......U/A..`.
0010  00 00 00 20 3a ff fe c0 00 00 00 00 00 01 02 0d   ... :...........
0020  9d ff fe 55 2f 41 ff 02 00 00 00 00 00 00 00 00   ...U/A..........
0030  00 01 ff 00 00 03 87 00 e1 ce 00 00 00 00 fe c0   ................
0040  00 00 00 00 ff ff 00 00 00 00 00 00 00 03 01 01   ................
0050  00 0d 9d 55 2f 41                                 ...U/A

No.     Time        Source                Destination           Protocol
Info
     12    17.460285          fec0::1:20d:9dff:fe55:2f41    ff02::1:ff00:2
ICMPv6   Neighbor solicitation

Frame 12 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Feb  7, 2005 20:51:09.529301000
    Time delta from previous packet: 0.000055000 seconds
    Time since reference or first frame: 17.460285000 seconds
    Frame Number: 12
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 33:33:ff:00:00:02
    Destination: 33:33:ff:00:00:02 (IPv6-Neighbor-Discovery_ff:00:00:02)
    Source: 00:0d:9d:55:2f:41 (10.0.1.1)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fec0::1:20d:9dff:fe55:2f41
    Destination address: ff02::1:ff00:2
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0xe1d0 (correct)
    Target: fec0:0:0:ffff::2
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41

0000  33 33 ff 00 00 02 00 0d 9d 55 2f 41 86 dd 60 00   33.......U/A..`.
0010  00 00 00 20 3a ff fe c0 00 00 00 00 00 01 02 0d   ... :...........
0020  9d ff fe 55 2f 41 ff 02 00 00 00 00 00 00 00 00   ...U/A..........
0030  00 01 ff 00 00 02 87 00 e1 d0 00 00 00 00 fe c0   ................
```

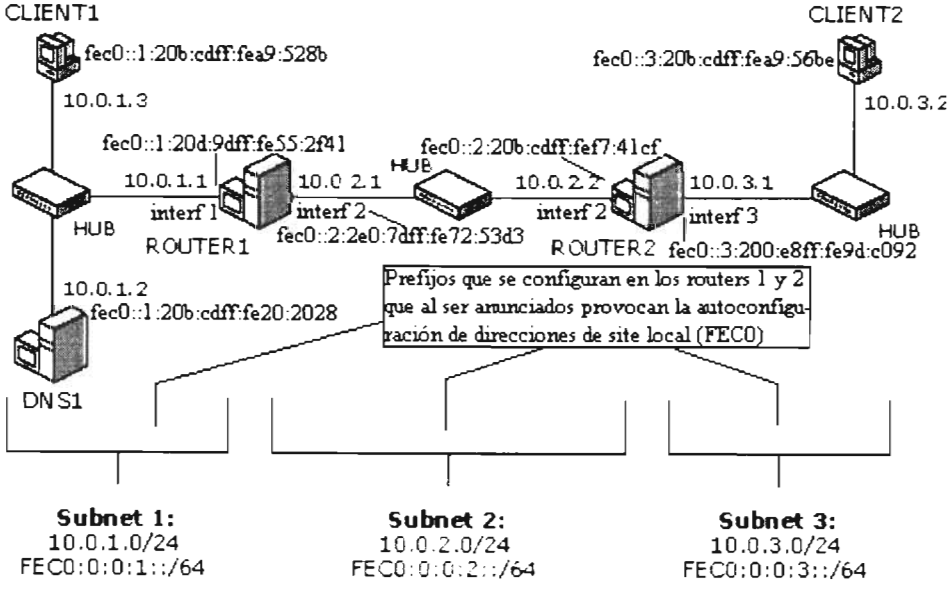
```
0040  00 00 00 00 ff ff 00 00 00 00 00 00 00 02 01 01   ................
0050  00 0d 9d 55 2f 41                                  ...U/A

No.     Time        Source                Destination           Protocol
Info
    13   17.460386          fec0::1:20d:9dff:fe55:2f41   ff02::1:ff00:1
ICMPv6   Neighbor solicitation

Frame 13 (86 bytes on wire, 86 bytes captured)
    Arrival Time: Feb  7, 2005 20:51:09.529402000
    Time delta from previous packet: 0.000101000 seconds
    Time since reference or first frame: 17.460386000 seconds
    Frame Number: 13
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 33:33:ff:00:00:01
    Destination: 33:33:ff:00:00:01 (IPv6-Neighbor-Discovery_ff:00:00:01)
    Source: 00:0d:9d:55:2f:41 (10.0.1.1)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fec0::1:20d:9dff:fe55:2f41
    Destination address: ff02::1:ff00:1
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0xe1d2 (correct)
    Target: fec0:0:0:ffff::1
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41

0000  33 33 ff 00 00 01 00 0d 9d 55 2f 41 86 dd 60 00   33.......U/A..`.
0010  00 00 00 20 3a ff fe c0 00 00 00 00 00 01 02 0d   ... :...........
0020  9d ff fe 55 2f 41 ff 02 00 00 00 00 00 00 00 00   ...U/A..........
0030  00 01 ff 00 00 01 87 00 e1 d2 00 00 00 00 fe c0   ................
0040  00 00 00 00 ff ff 00 00 00 00 00 00 00 01 01 01   ................
0050  00 0d 9d 55 2f 41                                  ...U/A
```

Podemos ver como las solicitudes de vecino son hechas por multicast **ff02::1:ff55:2f41** con terminación 55:2f41y posteriormente es recibida una respuesta del destino con la dirección correspondiente. Estas direcciones de link local se autoconfiguran cuando no se tienen los routers que hacen el anunciamiento de prefijo por lo que los hosts deben poseer una dirección local a su enlace.

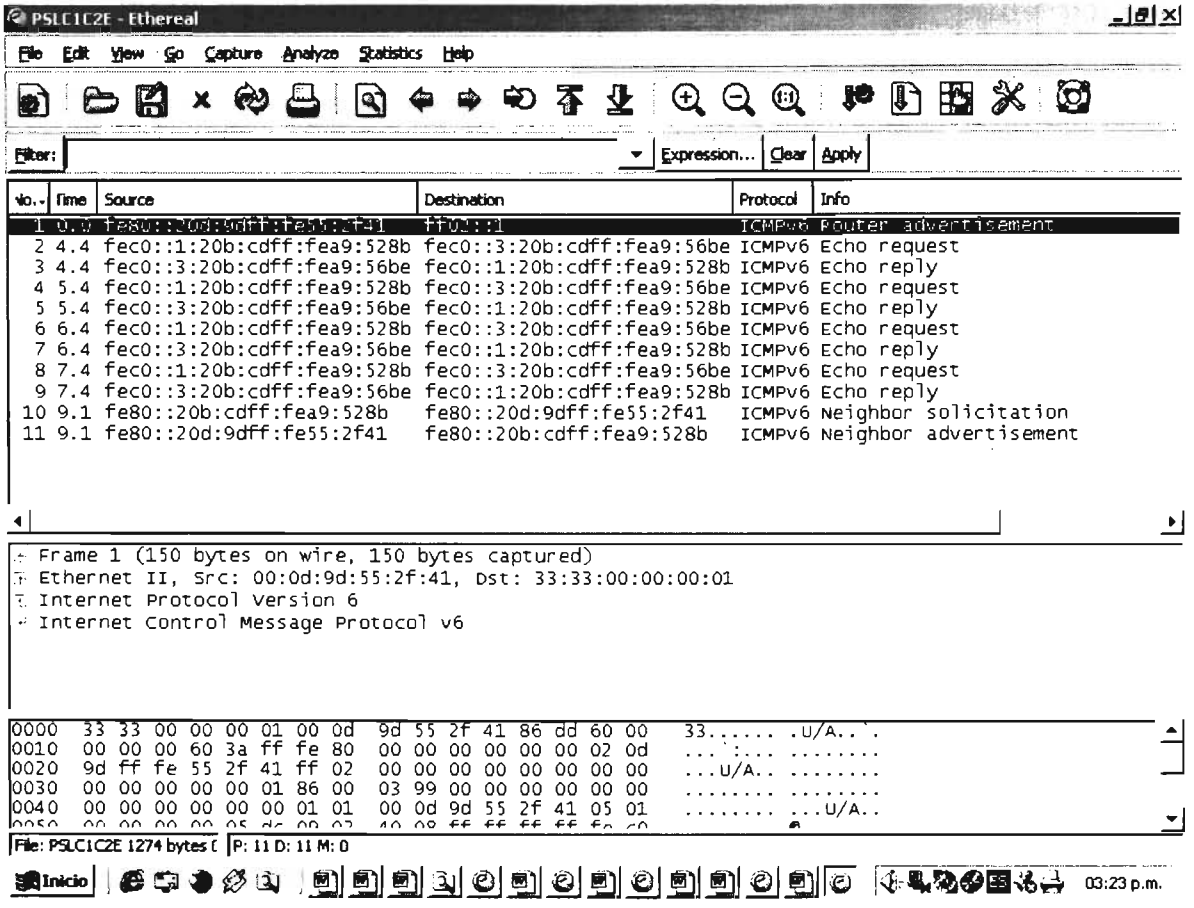
Cuando se tienen algún tipo de prefijo en una subred es importante que el router anuncie este prefijo para que todos los hosts conectados a la misma subred del router usen ese prefijo para autoconfigurar una dirección que tenga el mismo prefijo que el router, para que de esta manera todos los hosts pertenecientes a la misma subred se puedan comunicar sin

necesidad de configuración manual de la dirección a la vez de que manejan el mismo segmento en el cual están conectados.

- Anunciamiento de router.
  Para comprobar el anunciamiento que se hace en IPv6 del prefijo por parte del router tenemos el ejemplo del siguiente paquete donde un tenemos un router que realiza el anunciamiento de su prefijo FEC0, este paquete se capturo en el esquema de las pruebas con direcciones de site local:



Paquete de anunciamiento de router capturado con ethereal en cliente1:




```
No.     Time        Source                Destination           Protocol
Info
      1 0.000000    fe80::20d:9dff:fe55:2f41 ff02::1              ICMPv6
Router advertisement

Frame 1 (150 bytes on wire, 150 bytes captured)
    Arrival Time: Feb  2, 2005 10:02:49.309807000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 150 bytes
    Capture Length: 150 bytes
Ethernet II, Src: 00:0d:9d:55:2f:41, Dst: 33:33:00:00:00:01
    Destination: 33:33:00:00:00:01 (IPv6-Neighbor-Discovery_00:00:00:01)
    Source: 00:0d:9d:55:2f:41 (HewlettP_55:2f:41)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 96
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::20d:9dff:fe55:2f41
    Destination address: ff02::1
Internet Control Message Protocol v6
```

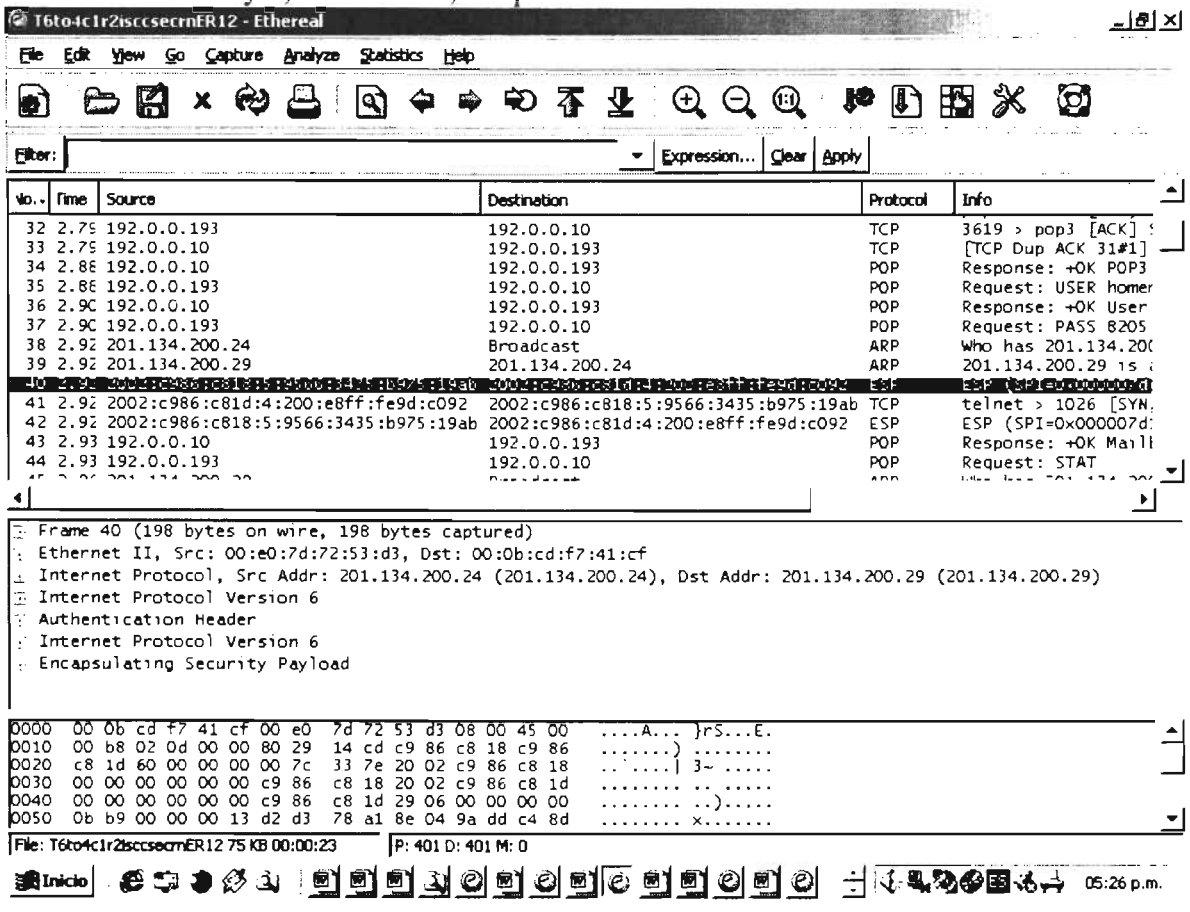
```
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x0399 (correct)
    Cur hop limit: 0
    Flags: 0x00
        0... .... = Not managed
        .0.. .... = Not other
        ..0. .... = Not Home Agent
        ...0 0... = Router preference: Medium
    Router lifetime: 0
    Reachable time: 0
    Retrans time: 0
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:0d:9d:55:2f:41
    ICMPv6 options
        Type: 5 (MTU)
        Length: 8 bytes (1)
        MTU: 1500
    ICMPv6 options
        Type: 9 (Unknown)
        Length: 16 bytes (2)
    ICMPv6 options
        Type: 9 (Unknown)
        Length: 16 bytes (2)
    ICMPv6 options
        Type: 3 (Prefix information)
        Length: 32 bytes (4)
        Prefix length: 64
        Flags: 0xc0
            1... .... = Onlink
            .1.. .... = Auto
            ..0. .... = Not router address
            ...0 .... = Not site prefix
        Valid lifetime: 0xffffffff
        Preferred lifetime: 0xffffffff
        Prefix: fec0:0:0:1::
```

```
0000  33 33 00 00 00 01 00 0d 9d 55 2f 41 86 dd 60 00   33.......U/A..`.
0010  00 00 00 60 3a ff fe 80 00 00 00 00 00 00 02 0d   ...`:...........
0020  ff ff fe 55 2f 41 ff 02 00 00 00 00 00 00 00 00   ...U/A..........
0030  00 01 00 00 00 01 86 00 03 99 00 00 00 00 00 00   ................
0040  00 00 00 00 00 00 01 01 00 0d 9d 55 2f 41 05 01   ...........U/A..
0050  00 00 00 00 05 dc 09 02 40 08 ff ff ff ff fe c0   ........@.......
0060  00 00 00 00 00 03 09 02 40 08 ff ff ff ff fe c0   ........@.......
0070  00 00 00 00 00 02 03 04 40 c0 ff ff ff ff ff ff   ........@.......
0080  00 01 00 00 00 00 fe c0 00 00 00 00 00 01 00 00   ................
0090  00 00 00 00 00 00                                 ......
```

Podemos ver que el anunciamiento que el router realiza es del tipo multicast **Destination address: ff02::1** y dentro de las opciones de ICMPv6 manda el prefijo el cual será usado por el host para autoconfigurar su dirección IPv6 mediante este prefijo y la dirección MAC del host.

- IPv6 permite la encapsulación de IPv6 en IPv6 (tunneling).
  Esto se hace con un valor 41 para el campo Next Header. El paquete IPv6 encapsulado puede tener sus propias EHs. Los routers no deberían agregar EHs a los paquetes. Si no encapsularlos en paquetes propios (fragmentados, si hace falta) ya que el tamaño de cada paquete se ha calculado en el nodo originador para que se ajuste al PMTU.

Esta encapsulación de IPv6 en IPv6 lo podemos comprobar en la captura de un paquete donde se configuro la seguridad del cliente1 hasta el router2, pasando por un túnel AH entre los routers 1 y 2, así tenemos, esa pantalla:




```
No.     Time        Source                Destination           Protocol
Info
     41     2.925804                    2002:c986:c818:5:9566:3435:b975:19ab
2002:c986:c81d:4:200:e8ff:fe9d:c092 ESP      ESP (SPI=0x000007d1)

Frame 40 (198 bytes on wire, 198 bytes captured)
    Arrival Time: Feb 25, 2005 16:46:40.479845000
    Time delta from previous packet: 2.925804000 seconds
    Time since reference or first frame: 2.925804000 seconds
    Frame Number: 40
    Packet Length: 198 bytes
    Capture Length: 198 bytes
Ethernet II, Src: 00:e0:7d:72:53:d3, Dst: 00:0b:cd:f7:41:cf
    Destination: 00:0b:cd:f7:41:cf (201.134.200.29)
    Source: 00:e0:7d:72:53:d3 (201.134.200.24)
    Type: IP (0x0800)
```

```
Internet Protocol, Src Addr: 201.134.200.24 (201.134.200.24), Dst Addr:
201.134.200.29 (201.134.200.29)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 184
    Identification: 0x020d (525)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
    Header checksum: 0x14cd (correct)
    Source: 201.134.200.24 (201.134.200.24)
    Destination: 201.134.200.29 (201.134.200.29)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 124
    Next header: AH (0x33)
    Hop limit: 126
    Source address: 2002:c986:c818::c986:c818
    Destination address: 2002:c986:c81d::c986:c81d
Authentication Header
    Next Header: IPv6 (0x29)
    Length: 32
    SPI: 0x00000bb9
    Sequence: 19
    ICV
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 52
    Next header: ESP (0x32)
    Hop limit: 127
    Source address: 2002:c986:c818:5:9566:3435:b975:19ab
    Destination address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
Encapsulating Security Payload
    SPI: 0x000007d1
    Sequence: 29
    Data (44 bytes)

0000  00 0b cd f7 41 cf 00 e0 7d 72 53 d3 08 00 45 00   ....A...}rS...E.
0010  00 b8 02 0d 00 00 80 29 14 cd c9 86 c8 18 c9 86   .......)........
0020  c8 1d 60 00 00 00 00 7c 33 7e 20 02 c9 86 c8 18   ..`....|3~ .....
0030  00 00 00 00 00 00 c9 86 c8 18 20 02 c9 86 c8 1d   .......... .....
0040  00 00 00 00 00 00 c9 86 c8 1d 29 06 00 00 00 00   ..........).....
0050  0b b9 00 00 00 13 d2 d3 78 a1 8e 04 9a dd c4 8d   ........x.......
0060  78 a3 9b ad 67 4b 00 00 00 00 60 00 00 00 00 34   x...gK....`....4
0070  32 7f 20 02 c9 86 c8 18 00 05 95 66 34 35 b9 75   2. ........f45.u
```

```
0080  19 ab 20 02 c9 86 c8 1d 00 04 02 00 e8 ff fe 9d   .. ..............
0090  c0 92 00 00 07 d1 00 00 00 1d 04 02 00 17 b1 ad   ................
00a0  8f 51 00 00 00 00 60 02 40 00 68 e4 00 00 02 04   .Q....`.@.h.....
00b0  05 a0 01 02 02 06 4a e9 d2 92 74 a2 ca 35 89 cd   ......J...t..5..
00c0  52 f9 b5 2f 40 4c                                 R../@L
```

Podemos observar que se cumple que IPv6 puede ser encapsulado dentro de IPv6 ya que tenemos un encabezado de IPv6 para el encapsulamiento del telnet con ESP el cual tiene como direcciones fuente y destino las siguientes:
Source address: 2002:c986:c818:5:9566:3435:b975:19ab
Destination address: 2002:c986:c81d:4:200:e8ff:fe9d:c092
Este paquete esta encapsulado dentro de un encabezado de IPv6 que hace pasar el trafico por un túnel de r1 a r2 con autentificación de encabezado con las siguientes direcciones fuente y destino:
Source address: 2002:c986:c818::c986:c818
Destination address: 2002:c986:c81d::c986:c81d
Podemos ver claramente que IPv6 esta encapsulado dentro de IPv6.

- Autoconfiguración de direcciones.
  IPv6 contiene varias formas de autoconfiguración como la configuración Plug and Play de direcciones de nodos sobre una red aislada gracias a las características de DHCP. Así esta característica proporciona una asignación dinámica de direcciones IPv6. La autoconfiguración de direcciones es simple en direcciones tipo Aggregatable Global Unicast donde los 64 bits superiores son establecidos por un mensaje desde el router y los 64 bits más bajos son establecidos por la dirección MAC (en formato EUI-64). De esta forma el largo del prefijo de la subred es de 64 por lo que la mascara de red ya no implica preocupación alguna. Asimismo el largo del prefijo no depende del numero de hosts por lo que la asignación es más simple. Esta característica de autoconfiguración también permite que la renumeración en caso de cambiar de proveedor de Internet sea más fácil.

Pudimos comprobar que estas características de autoconfiguración de direcciones se cumplen perfectamente, ya que en primer lugar los hosts aun sin recibir un anunciamiento de prefijo de algún router y aunque no tengan alguna dirección IPv4 configurada, con el simple hecho de tener el protocolo IPv6 instalado pueden autonconfigurar una dirección IPv6 en formato EUI-64, es decir tomando la dirección MAC de su tarjeta Ethernet pueden autoconfigurar una dirección IPv6:

Anexo A Configuración del cliente1

Sin configurar alguna dirección IPv4 se instala IPv6 y el comando ipconfig arroja la siguiente información:

```
C:\Documents and Settings\cliente1>ipconfig
Configuración IP de Windows
Adaptador Ethernet Conexión de área local :
        Sufijo de conexión específica DNS :
        Dirección IP de autoconfiguración : 169.254.3.129
        Máscara de subred . . . . . : 255.255.0.0
        Dirección IP. . . . . : fe80::20b:cdff:fea9:528b%5
        Puerta de enlace predeterminada :

Adaptador de túnel Teredo Tunneling Pseudo-Interface :
        Sufijo de conexión específica DNS :
```

Dirección IP. . . . . : **fe80::5445:5245:444f%4**
Puerta de enlace predeterminada :

Adaptador de túnel Automatic Tunneling Pseudo-Interface :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : **fe80::5efe:169.254.3.129%2**
Puerta de enlace predeterminada :

C:\Documents and Settings\cliente1>

También pudimos constatar que cada nodo autoconfigura una dirección de bucle invertido mas comúnmente conocidas como de loopback con direcccón ::1 o fe80::1.

Podemos observar que las direcciones de link local se autoconfiguran sin tener alguna dirección IPv4 configurada manualmente.

Podemos ver que las direcciones IPv6 se autoconfiguran en base a la dirección MAC y un prefijo recibido o no. Si no reciben un anunciamiento del router se autoconfigura la dirección IPv6 con un prefijo link local FE80, cuando reciben anunciamiento de router autoconfiguran la dirección IPv6 con la dirección MAC y el prefijo recibido ya sea link local (FE80), site local (FEC0), isatap (FE80::5efe), temporal (3FFE), global (2002).

La autoconfiguración funciona correctamente, puesto que en todas las pruebas realizadas en los hosts nunca se configuro alguna dirección IPv6 en forma manual, únicamente se configuraron ya sea rutas estáticas con prefijos, direcciones IPv4 publicas configuradas e ICS compartido lo cual por anunciamiento provocaba la configuración de las direcciones IPV6 con las que se hicieron las pruebas de conectividad.

En las pruebas realizadas también pudimos trabajar con los diferentes tipos de direcciones que se pueden configurar en un nodo, todas y cada una de ellas fueron configuradas automáticamente, con el anunciamiento del prefijo de los routers y el identificador físico de la tarjeta de red de cada nodo, pudimos darnos cuenta que cada nodo puede mantener varias direcciones de distinto tipo en cada una de sus interfaces, es decir pueden tener una dirección de link local, de site local, temporales, globales al mismo tiempo en su interfaz de área local y funcionan todas sin afectarse entre sí.

En el caso de las direcciones de link local estas se configuran inmediatamente al instalar el protocolo IPv6.

Las direcciones de site local se autoconfiguran después de indicar a los routers el prefijo que usara cada una de las interfaces de area local instaladas, posteriormente el router anuncia esos prefijos y los nodos combinan el prefijo que les llega con el identificador EUI-64 para formar la dirección IPv6 de site local.

Las direcciones temporales y globales se configuran de la misma manera pero asignando primeramente direcciones públicas a las interfaces de los routers que ven hacia Internet y compartiendo su conexión a Internet, así los routers anuncian prefijos en base a una conversión hexadecimal de la dirección publica configurada a la que se le antepone el prefijo 3ffe o 2002.

Las direcciones para realizar túneles de IPv6 dentro de IPv4 configuran las direcciones IPv6 en base a las direcciones privadas o publicas que tengan configuradas en su interfaz local, por lo cual para que estas funcionen la infraestructura de ruteo de IPv4 debe trabajar correctamente para que de este modo el nodo pueda ver a su nodo destino por IPv4 primeramente ya que si esto no se cumple las direcciones de tunelización no funcionaran.

De las pruebas realizadas tenemos los siguientes listados de las direcciones que autonfiguraron los nodos en cada esquema de laboratorio de pruebas:

Nodo	Dirección link local	Prefijo de red	ID de interface=EUI-64
Cliente1	**fe80::20b:cdff:fea9:528b%ldif**	**Fe80::/64**	**20b:cdff:fea9:528b**
DNS	**fe80::20b:cdff:fe20:2028%ldif**	**Fe80::/64**	**20b:cdff:fe20:2028**
Intf 1 router1	**fe80::20d:9dff:fe55:2f41%ldif**	**Fe80::/64**	**20d:9dff:fe55:2f41**
Intf 2 router 1	**fe80::2e0:7dff:fe72:53d3%ldif**	**Fe80::/64**	**2e0:7dff:fe72:53d3**
Intf 2 router 2	**fe80::20b:cdff:fef7:41cf%ldif**	**Fe80::/64**	**20b:cdff:fef7:41cf**
Intf 3 router 2	**fe80::200:e8ff:fe9d:c092%ldif**	**Fe80::/64**	**200:e8ff:fe9d:c092**
Cliente 2	**fe80::20b:cdff:fea9:56be%ldif**	**Fe80::/64**	**20b:cdff:fea9:56be**

Prefijo de link local
Fe80::/10
Fe80::/10
Fe80::/10
Fe80::/10
Fe80::/10
Fe80::/10
Fe80::/10

Estas son direcciones de intraenlace configuradas por el nodo en ausencia de ruteador.
Con estas direcciones el prefijo es fe80/10 (fe80=1111 1110 10), los primeros diez bits nos indican el tipo de dirección que es link local.
Podríamos decir que se usan direcciones link local puras sin subneting ya que el prefijo usado es el de link local asignado por default fe80 con 0´s en los 3 campos de 16 bits restantes.

Para la parte de pruebas de site local las direcciones que se autoconfiguraron fueron:

Nodo	Dirección unicast de site local	Prefijo de red	ID de interface=EUI-64
Cliente1	**fec0::1:20b:cdff:fea9:528b**	**Fec0:0:0:1::/64**	**20b:cdff:fea9:528b**
DNS	**fec0::1:20b:cdff:fe20:2028**	**Fec0:0:0:1::/64**	**20b:cdff:fe20:2028**
Intf 1 router1	**fec0::1:20d:9dff:fe55:2f41**	**Fec0:0:0:1::/64**	**20d:9dff:fe55:2f41**
Intf 2 router 1	**fec0::2:2e0:7dff:fe72:53d3**	**Fec0:0:0:2::/64**	**2e0:7dff:fe72:53d3**
Intf 2 router 2	**fec0::2:20b:cdff:fef7:41cf**	**Fec0:0:0:2::/64**	**20b:cdff:fef7:41cf**
Intf 3 router 2	**fec0::3:200:e8ff:fe9d:c092**	**Fec0:0:0:3::/64**	**200:e8ff:fe9d:c092**
Cliente 2	**fec0::3:20b:cdff:fea9:56be**	**Fec0:0:0:3::/64**	**20b:cdff:fea9:56be**

Prefijo de site local	Subnet ID
Fec0::/10	**1::/16**
Fec0::/10	**1::/16**
Fec0::/10	**1::/16**
Fec0::/10	**2::/16**
Fec0::/10	**2::/16**
Fec0::/10	**3::/16**
Fec0::/10	**3::/16**

Todas las direcciones son de interenlace configuradas con la obtención del prefijo por anunciamiento de router concatenado al identificador EUI_64
Con estas direcciones el prefijo es fec0/10 (fec0=1111 1110 11), los primeros diez bits nos indican el tipo de dirección que es site local.
En este caso debido a que se usaron en un laboratorio que estaba dentro de un sitio formado con subredes diferentes, no se uso el prefijo puro de fec0, ya que se realizo subnneting en IPv6 por lo cual podemos manejar el prefijo como aumentado a 64 bits que se representa como: fec0:0:0:1::/64, fec0:0:0:2::/64, fec0:0:0:3::/64. Es decir tenemos tres subredes con prefijo fec0: fec0:0:0:1::/64= subred 1 con prefijo fec0::/10, fec0:0:0:2::/64= subred 2 con prefijo fec0::/10 y fec0:0:0:3::/64= subred 3 con prefijo fec0::/10.

Para la parte de pruebas con direcciones ISATAP se obtuvieron las siguientes direcciones:

Nodo	Dirección ISATAP
Cliente1	**fe80::5efe:10.0.1.3%2**
DNS	**fe80::5efe:10.0.1.2%2**
Intf 1 router1	**fe80::5efe:10.0.1.1%2**
Intf 2 router 1	**fe80::5efe:10.0.2.1%2**
Intf 2 router 2	**fe80::5efe:10.0.2.2%2**
Intf 3 router 2	**fe80::5efe:10.0.3.1%2**
Cliente 2	**fe80::5efe:10.0.3.2%2**

Como vemos por los primeros 16 bits estas son direcciones del tipo link local (fe80), la parte de 5efe es para indicar al sistema que se realice un encapsulamiento en la dirección IPv4 que le sigue a los dos puntos.

Para las pruebas con direcciones temporales las direcciones autoconfiguradas son :

Nodo	Dirección 6to4 temporal	Prefijo de red	ID de interface=EUI-64
Cliente1	**3ffe:ffff:0:1:20b:cdff:fea9:528b**	**3ffe:ffff:0:1::/64**	**20b:cdff:fea9:528b**
DNS	**3ffe:ffff:0:1:20b:cdff:fe20:2028**	**3ffe:ffff:0:1::/64**	**20b:cdff:fe20:2028**
Intf 1 router1	**3ffe:ffff:0:1:20d:9dff:fe55:2f41**	**3ffe:ffff:0:1::/64**	**20d:9dff:fe55:2f41**
Intf 2 router 1	**3ffe:ffff:0:2:2e0:7dff:fe72:53d3**	**3ffe:ffff:0:2::/64**	**2e0:7dff:fe72:53d3**
Intf 2 router 2	**3ffe:ffff:0:2:20b:cdff:fef7:41cf**	**3ffe:ffff:0:2::/64**	**20b:cdff:fef7:41cf**
Intf 3 router 2	**3ffe:ffff:0:3:200:e8ff:fe9d:c092**	**3ffe:ffff:0:3::/64**	**200:e8ff:fe9d:c092**
Cliente 2	**3ffe:ffff:0:3:20b:cdff:fea9:56be**	**3ffe:ffff:0:3::/64**	**20b:cdff:fea9:56be**

Estas son direcciones del tipo globales temporales por los dos primeros octetos 3ffe, pero no se uso el prefijo temporal global puro sino que se hizo un subnetting donde los prefijos son:
3ffe:ffff:0:1::/64, 3ffe:ffff:0:2::/64, 3ffe:ffff:0:3::/64

Para la prueba de las direcciones compatibles las direcciones que se autoconfiguraron son:

Nodo	Dirección v4-compatible	Prefijo de red
Cliente1	::10.0.1.3	::/96
DNS	::10.0.1.2	::/96
Intf 1 router1	::10.0.1.1	::/96
Intf 2 router 1	::10.0.2.1	::/96
Intf 2 router 2	::10.0.2.2	::/96
Intf 3 router 2	::10.0.3.1	::/96
Cliente 2	::10.0.3.2	::/96

Como se puede ver estas son direcciones con prefijo compuesto de puros ceros es decir: ::/96

En el esquema para las pruebas con direcciones 6to4 globales donde se configuraron las direcciones IPv4 publicas de 182.0.0.81 y 192.0.0.82 en las interfaces 2 de los routers 2 las direcciones que se autoconfiguraron al anunciarse estas direcciones fueron:

Nodo	Dirección (6to4) unicast global	Prefijo de red	ID de interface=EUI-64
Cliente1	2002:c000:51:5:20b:cdff:fea9:528b	2002:c000:51::/48	20b:cdff:fea9:528b
DNS	2002:c000:51:5:20b:cdff:fe20:2028	2002:c000:51::/48	20b:cdff:fe20:2028
Intf 1 router1	2002:c000:51:5:1:20d:9dff:fe55:2f41	2002:c000:51::/48	20d:9dff:fe55:2f41
Intf 2 router 1	2002:c000:51::c000:51	2002:c000:51::/48	2e0:7dff:fe72:53d3
Intf 2 router 2	2002:c000:52::c000:52	2002:c000:52::/48	20b:cdff:fef7:41cf
Intf 3 router 2	2002:c000:52:4:200:e8ff:fe9d:c092	2002:c000:52::/48	200:e8ff:fe9d:c092
Cliente 2	2002:c000:52:4:20b:cdff:fea9:56be	2002:c000:52::/48	20b:cdff:fea9:56be

Prefijo indicador de dirección global	Prefijo de ruteo global	Subnet ID
2000::/3	2:c000:51::/45	5::/16
2000::/3	2:c000:51::/45	5::/16
2000::/3	2:c000:51::/45	5::/16
2000::/3	2:c000:51::/45	
2000::/3	2:c000:52::/45	
2000::/3	2:c000:52::/45	4::/16
2000::/3	2:c000:52::/45	4::/16

Podemos ver que en los routers se autoconfigura el prefijo de direcciones 6to4 unicast globales de agregación 2002 en los dos primeros octetos que empiezan con el identificador de direcciones unicast globales de 001, los siguientes campos 2 y 3 son la representación hexadecimal de la dirección IPv4 publica configurada en la interfaz publica del router 2 es decir 192.0.0.81=c000:51 y 192.0.0.82=c000:52, estos junto con los últimos 13 bits del primer campo hexadecimal forman el prefijo de ruteo global y el cuarto campo de dos octetos es el identificador de subred que en este caso es el numero identificador de la interfaz donde se configuro la dirección IPv4 publica.

En la prueba con direcciones IPv4 publicas de diferentes subred se configuraron las direcciones 192.0.0.147 y 192.0.100.63 en los routers 2 con lo que las direcciones IPv6 autoconfiguradas fueron:

Nodo	Dirección 6to4 global	Prefijo de red	ID de interface=EUI-64
Cliente1	**2002:c000:93:5:20b:cdff:fea9:528b**	**2002:c000:93::/48**	**20b:cdff:fea9:528b**
DNS	**2002:c000:93:5:20b:cdff:fe20:2028**	**2002:c000:93::/48**	**20b:cdff:fe20:2028**
Intf1 router1	**2002:c000:93:5:1:20d:9dff:fe55:2f41**	**2002:c000:93::/48**	**20d:9dff:fe55:2f41**
Intf2 router 1	**2002:c000:93::c000:93**	**2002:c000:93::/48**	**2e0:7dff:fe72:53d3**
Intf2 router 2	**2002:c000:643f::c000:643f**	**2002:c000:643f::/48**	**20b:cdff:fef7:41cf**
Intf3 router 2	**2002:c000:643f:4:200:e8ff:fe9d:c092**	**2002:c000:643f::/48**	**200:e8ff:fe9d:c092**
Cliente 2	**2002:c000:643f:4:20b:cdff:fea9:56be**	**2002:c000:643::/48**	**20b:cdff:fea9:56be**

Tenemos direcciones 6to4 globales formadas con la combinación de 2002 con la representación hexadecimal de: 192.0.0.147=c000:93 y 192.0.100.40=c000:643f

En el esquema de las subredes 1 y 3 conectadas a Internet mediante dos direcciones IPv4 publicas homologadas se autoconfiguraron las siguientes direcciones:

Nodo	Dirección 6to4 global	Prefijo de red	ID de interface=EUI-64
Cliente1	**2002:c986:c818:b:20b:cdff:fea9:528b**	**2002:c986:c818::/48**	**20b:cdff:fea9:528b**
DNS	**2002:c986:c818:b:20b:cdff:fe20:2028**	**2002:c986:c818::/48**	**20b:cdff:fe20:2028**
Intf 1 router1	**2002:c986:c818:b:1:20d:9dff:fe55:2f41**	**2002:c986:c818::/48**	**20d:9dff:fe55:2f41**
Intf 2 router 1	**2002:c986:c818::c986:c818**	**2002:c986:c818::/48**	**2e0:7dff:fe72:53d3**
Intf 2 router 2	**2002:c986:c81d::c986:c81d**	**2002:c986:c81d::/48**	**20b:cdff:fef7:41cf**
Intf 3 router 2	**2002:c986:c81d:4:200:e8ff:fe9d:c092**	**2002:c986:c81d::/48**	**200:e8ff:fe9d:c092**
Cliente 2	**2002:c986:c81d:4:20b:cdff:fea9:56be**	**2002:c986:c81d::/48**	**20b:cdff:fea9:56be**

Tenemos el prefijo de una dirección global 6to4 2002 con la representación hexadecimal de las direcciones IPv4: 201.134.200.24=c986:c818 y 202.134.200.29=c986:c81d

En el ultimo esquema usado con la subred 1 conectada a Internet por medio de un enlace de prodigy infinitum de 512 kbps y la subred 3 por medio de un enlace dedicado a UNINET de 2 Mbps. tenemos las siguientes direcciones:

Nodo	Dirección 6to4 global	Prefijo de red	ID de interface=EUI-64
Cliente1	**2002:c980:1cb4:5:20b:cdff:fea9:528b**	**2002:c980:1cb4::/48**	**20b:cdff:fea9:528b**
DNS	**2002:c980:1cb4:5:20b:cdff:fe20:2028**	**2002:c980:1cb4::/48**	**20b:cdff:fe20:2028**
Intf 1 router1	**2002:c980:1cb4:5:1:20d:9dff:fe55:2f41**	**2002:c980:1cb4::/48**	**20d:9dff:fe55:2f41**
Intf 2 router 1	**2002:c980:1cb4::c980:1cb4**	**2002:c980:1cb4::/48**	**2e0:7dff:fe72:53d3**
Intf 2 router 2	**2002:c986:c81d::c986:c81d**	**2002:c986:c81d::/48**	**20b:cdff:fef7:41cf**
Intf 3 router 2	**2002:c986:c81d:4:200:e8ff:fe9d:c092**	**2002:c986:c81d::/48**	**200:e8ff:fe9d:c092**
Cliente 2	**2002:c986:c81d:4:20b:cdff:fea9:56be**	**2002:c986:c81d::/48**	**20b:cdff:fea9:56be**

Tenemos el prefijo de dirección 6to4 global 2002 y la representación hexadecimal de las direcciones IPv4 publicas dinámicas y fijas: 201.128.28.180=c980:1cb4, 201.134.200.29=c986:c81d

APÉNDICE B

Listado de RFCs relacionados a la estandarización de IPv6

Los protocolos de Internet son desarrollados mediante las peticiones para comentarios o RFC (Request For Comments) que se publican abiertamente. RFC es descrito por el IAB (Internet Architecture Board). La mayor fuente de RFCs es el IETF (Internet Engineering Task Force) organización subsidiaria del IAB. Sin embargo, cualquiera puede enviar un informe propuesto como RFC al editor de los RFCs.

Una vez que un RFC ha sido publicado, todas las revisiones y sustituciones se publican como nuevos RFCs. Se dice que un nuevo RFC que revisa o sustituye un RFC ya existente "actualiza" o "desfasa" a ese RFC. Asimismo, el RFC original es "actualizado" o "desfasado" por el nuevo. Por ejemplo el RFC 1521 se etiqueta del modo siguiente: "Deja obsoleto al RFC 1341; Actualizado por el RFC 1590". En consecuencia, nunca hay confusión sobre si dos personas se refieren a dos versiones distintas de un RFC,

Algunos RFCs se califican como documentos informativos mientras que otros describen protocolos de Internet. El IAB mantiene una lista de todos los RFCs que describen la pila de protocolos. A cada uno de ellos se le asigna un estado y un status.

Todos los protocolos de Internet pueden tener uno de los siguientes estados:

- Estándar

El IAB lo ha establecido como protocolo oficial de Internet. Se dividen en dos grupos:
Protocolo superiores, protocolos que se aplican a la totalidad de Internet.
Protocolos específicos de redes, generalmente especificaciones del funcionamiento de IP en tipos concretos de redes.

- Estándar provisional

El IAB está considerando activamente este protocolo como un posible protocolo estándar. Es deseable disponer de comentarios y pruebas exhaustivas cuantitativa y cualitativamente. Los comentarios y los resultados de las pruebas deberían enviarse al IAB. Existe la posibilidad de que se efectúen cambios en un protocolo estándar provisional antes de que se convierta en estándar.

- Propuesto como estándar.

Se trata de propuestas de protocolos que el IAB puede considerar para la estandarización en el futuro. Es deseable evaluar la implementación y la prueba sobre un gran número grupos. Es probable que el protocolo se someta a revisión.

- Experimental

Un sistema no debería implementar un protocolo experimental a menos que participe en el experimento y haya coordinado el uso que va a hacer del protocolo con el que lo ha desarrollado.

- Informativo

Los protocolos desarrollados por otras organizaciones de estándares, o distribuidores, o aquellos que por otras razones son ajenos a los propósitos del IAB, pueden ser publicados a conveniencia de la comunidad de Internet como protocolos informativos. En algunos casos el IAB puede recomendar el uso de estos protocolos en Internet.

- Histórico

Son protocolos con pocas posibilidades de convertirse alguna vez en estándar en Internet, bien porque han quedado desfasados por protocolos posteriores o debido a la falta de interés.

Definiciones del status de los protocolos:

- Requerido

Un sistema debe implementar los protocolos requeridos.

- Recomendado

Un sistema debería implementar un protocolo recomendado.

- Electivo

Un sistema puede o no implementar un protocolo electivo. La idea general es que si se va a implementar, debe hacerse exactamente como se define.

- Uso limitado.

Estos protocolos son usados en circunstancias específicas. Esto se puede deber a su estado experimental, naturaleza específica, funcionalidad limitada o estado histórico.

- No recomendado.

Estos protocolos no se recomiendan para el uso general. Esto se puede deber a su limitada funcionalidad, naturaleza específica, o a que su estado es experimental o histórico.

Estándares de Internet

Los estándares propuestos, provisionales, y los protocolos estándar figuran en el Internet Standards Track (Seguimiento de estándares de Internet). El seguimiento de estándares es controlado por el IESG (Internet Engineering Steering Group) del IETF.

Cuando un protocolo alcanza el estado de estándar, se le asigna un número de estándar (STD). El propósito del STD es indicar claramente que RFCs describen estándares de Internet. Los números STD referencian múltiples RFCs cuando la especificación de un estándar está repartida entre varios documentos. A diferencia de los RFCs, donde el número se refiere a un documento específico, los números STD no cambian cuando un estándar es actualizado. Sin embargo, los STD carecen de número de versión ya que todas las actualizaciones se hacen a través de RFCs y los RFCs son únicos. De este modo, para especificar sin ambigüedades a que estándar se refiere uno, el número de estándar y todos los RFCs que incluye deberían ser mencionados. Por ejemplo, el DNS (Domain Name System) tiene el STD 13, y se describe en los RFCs 1034 y 1035. Para referenciar un estándar, se debería usar una forma como "STD-13/RFC-1034/RFC-1035".

El RFC 1602 (Los procedimientos para estándares de Internet - Revisión 2) proporciona una descripción de los procedimientos para los estándares.

Para el seguimiento de algunos estándares, el status del RFC no siempre contiene suficiente información como para ser útil. Por ello se le añade un descriptor de aplicabilidad, dado bien en la forma de STD 1 en un RFC separado; este descriptor lo dan particularmente los protocolos de encaminamiento.

Cuatro estándares de Internet son de particular importancia:

STD 1 - Estándares de protocolo oficiales en Internet

STD 2 - Números asignados de Internet

STD 3 - Requerimientos de host

STD 4 - Requerimientos de pasarela

En la tabla siguiente tenemos una relación de los RFCs relacionados al tema de IPv6.

RFC	Obsoleto	Titulo	Categoría	Fecha	Autor
1752		Recomendación para el protocolo de siguiente generación IP	Standards track	Ene/ 1995	Universidad de Harvard
1809		Uso del campo etiqueta de flujo en IPv6	Informativo	Jun/ 1995	BBN
1828		Autenticación IP usando MD5 codificado	Standards track	Ago/ 1995	Piermont
1881		Administración de la asignación de direcciones IPv6	Informativo	Dic/ 1995	IAB e IESG
1883		Especificación del protocolo de Internet, versión 6 (IPv6)	Standards track	Dic/ 1995	Ipsilon Networks
1884		Arquitectura de direccionamiento IPv6	Standards track	Dic/ 1995	Ipsilon Networks, Xerox
1885		Especificación del protocolo de mensajes para el control de Internet (ICMPv6) para el protocolo de Internet (IPv6)	Standards track	Dic/ 1995	DEC, Xerox
1886		Extensiones DNS para el soporte de IPv6	Standards track	Dic/ 1995	Bellcore, Inria
1887		Arquitectura para la asignación de dirección Unicast IPv6	Informativo	Dic/ 1995	Cisco
1888		IPv6 y OSI NSAPs	Experimental	Ago/ 1996	DEC, CERN, ICL Network Systems, Datacraft Tech.
1897		Asignación de direcciones de prueba IPv6	Experimental	Ene/ 1996	Ipsilon Networks, ISI
1924		Representación compacta de direcciones IPv6	Informativo	Abr/ 1996	Univ. De Melbourne
1933		Mecanismos de Transición para Routers y Hosts IPv6	Standards track	Abr/ 1996	Sun Microsystems
1970		Descubrimiento de vecinos (Neighbor Discovery) para IPv6	Standards track	Ago/ 1996	IBM, SUN
1971		Autoconfiguración de dirección stateless IPv6	Standards track	Ago/ 1996	Bellcore, IBM
1972		Metodo para la transmisión de paquetes IPv6 sobre Ethernet	Standards track	Ago/ 1996	Fermilab
1981		Descubrimiento del MTU de la ruta para IPv6	Standards track	Ago/ 1996	DEC, Xerox
2019		Metodo para la transmisión de paquetes IPv6 sobre FDDI	Standards track	Oct/ 1996	Fermilab

2023		IPv6 sobre PPP	Standards track	Oct/ 1996	Bay Networks
2030	1769	Protocolo de tiempo de red simple para IPv4, IPv6 y OSI	Informativo	Oct/ 1996	Univ. de Delaware
2073		Formato de la dirección Unicat basado en proveedor IPv6	Standards track	Ene/ 1997	Cisco, Ipsilon, Xerox, ISI
2080		RIP para IPv6	Standards track	Ene/ 1997	Xylogics, Ipsilon Networks
2081		Aplicabilidad de RIPng para IPv6	Informativo	Ene/ 1997	Xylogics
2104		HMAC: Codificación llaveada para autenticación	Informativo	Feb/ 1997	IBM, UCSD
2133		Extensiones de la interfaz de sockets basicos para IPv6	Informativo	Abr/ 1997	Freegate, Bellcore, Digital
2147	Actua-liza a1883	TCP y UDP sobre datagramas gigantes (Jumbograms) IPv6	Standards track	May/ 1997	BSD Inc.
2185		Aspectos de ruteo de la transición IPv6	Informativo	Sep/ 1997	Cascade, Bay Networks
2260		Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor	Informativo	Ene/ 1998	Cisco
2283		Extensiones multiprotocolo para BGP-4	Standards track	Feb/ 1998	Cisco, Juniper Networks
2292		Sockets avanzados para la API IPv6	Informativo	Feb/ 1998	Altavista
2373	1884	Arquitectura de direccionamiento IPv6	Standards track	Jul/ 1998	Nokia, Cisco
2374	2073	Formato de la dirección Unicast de agregación global IPv6	Standards track	Jul/ 1998	Nokia, UUNET, Cisco
2375		Asignaciones de direcciones multicast IPv6	Informativo	Jul/ 1998	Ipsilon Networks, Cisco
2401	1825	Arquitectura de seguridad para el protocolo de Internet	Standards track	Nov/ 1998	BBN Corp., @ Home network
2402	1826	Cabecera de autenticación IP	Standards track	Nov/ 1998	BBN Corp., @ Home network
2403		Uso de HMAC-MD5-96 en ESP y AH	Standards track	Nov/ 1998	Cisco, NIST
2404		Uso de HMAC-SHA-1-96 dentro de ESP y AH	Standards track	Nov/ 1998	Cisco, NIST
2405		Algoritmo de cifrado DES-CBC para ESP	Standards track	Nov/ 1998	Cisco, Bay Networks
2406	1827	Encriptación de seguridad de la carga util (ESP) IP	Standards track	Nov/ 1998	BBN Corp., @ Home network

2407		IPSec para ISAKMP	Standards track	Nov/ 1998	Network Alchemy
2408		Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)	Standards track	Nov/ 1998	National Security Agency y Securify
2409		Intercambio de llaves por Internet (IKE)	Standards track	Nov/ 1998	Cisco
2410		Algoritmo de encripción nula y su uso con IPSec	Standards track	Nov/ 1998	NIST, BBN Corp.
2411		Seguridad IP	Informativo	Nov/ 1998	Bay Networks
2428		Extensiones FTP para IPv6 y NAT	Standards track	Sep/ 1998	Sterling software, Ohio Univ. Inner Net
2450		Propuesta de reglas de asignación TLA y NLA	Informativo	Dic/ 1998	Nokia
2451		Algoritmos de cifrado en modo CBC para ESP	Standards track	Nov/ 1998	Timestep, Cisco
2452		Base de información de administración (MIB) para TCP IPv6	Standards track	Dic/ 1998	Compaq
2454		MIB para UDP IPv6	Standards track	Dic/ 1998	Compaq
2460	1883	Especificación de protocolo de Internet versión 6 (IPv6)	Standards track	Dic/ 1998	Cisco, Nokia
2461	1970	Descubrimiento de vecinos (Neighbor Discovery) para IPv6	Standards track	Dic/ 1998	IBM, SUN, Daydreamer
2462	1971	Autoconfiguración stateless de direcciones IPv6	Standards track	Dic/ 1998	Bellcore, IBM
2463	1865	Especificación del protocolo de mensajes para el control de Internet (ICMPv6) para el protocolo de Internet (IPv6)	Standards track	Dic/ 1998	Lucent, Cisco
2464	1972	Transmisión de paquetes IPv6 sobre redes Ethernet	Standards track	Dic/ 1998	Fermilab
2465		MIB para IPv6. Convenciones tectuales y grupo general	Standards track	Dic/ 1998	Bay Networks
2466		MIB para IPv6: Grupo ICMPv6	Standards track	Dic/ 1998	Bay Networks
2467	2019	Transmisión de paquetes IPv6 sobre redes FDDI	Standards track	Dic/ 1998	Fermilab
2470		Transmisión de paquetes IPv6 sobre redes Token Ring	Standards track	Dic/ 1998	Fermilab, IBM
2471	1897	Asignación de direcciones de	Experiment	Dic/	Nokia, LBLN, ISI

		prueba IPv6	al	1998	
2472	2023	IPv6 sobre PPP	Standards track	Dic/ 1998	Bay Networks
2473		Especificación genérica para el encapsulamiento (tunneling) de paquetes en IPv6	Standards track	Dic/ 1998	Lucent, Cisco
2474	1455, 1349	Definición del campo de servicios diferenciados en IPv4 e IPv6	Standards track	Dic/ 1998	Cisco, Torrent Networking, EMC Corp.
2491		IPv6 sobre redes de Acceso Múltiple Sin Broadcast	Standards track	Ene/ 1999	Lucent, Digital, Compaq
2492		IPv6 sobre redes ATM	Standards track	Ene/ 1999	Lucent, Digital, Brigth Tiger
2497		Transmisión de paquetes IPv6 sobre redes ARCnet	Standards track	Ene/ 1999	Proyecto NetBSD
2507		Compresión del encabezado IP	Standards track	Feb/ 1999	Lulea university Tech.
2508		Compresión de encabezados IP/UDP/RTP para enlaces serials de baja velocidad	Standards track	Feb/ 1999	Cisco
2509		Compresión de encabezado IP sobre PPP	Standards track	Feb/ 1999	Effnet, Cisco
2526		Direcciones de subredes anycast IPv6 reservadas	Standards track	Mar/ 1999	Carnegie university, Cisco
2529		Transmisión de IPv6 sobre dominios IPv4 sin tuneles explicitos	Standards track	Mar/ 1999	IBM, 3COM
2545		Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6	Standards track	Mar/ 1999	Cisco, Inria
2546		Practicas de ruteo en 6BONE	Informativo	Mar/ 1999	IMAG, AT&T
2553	2133	Extensiones de la interfaz de socket basico para IPv6	Informativo	Mar/ 1999	Freegate, Bellcore, Compaq
2590		Especificación de la transmisión de paquetes IPv6 sobre redes Frame Relay	Standards track	May/ 1999	Lucent, Ascend
2663		Consideraciones y terminología de IP NAT	Informativo	Ago/ 1999	Lucent Technologies
2675	2147	Datagramas gigantes (Jumbograms)	Standards track	Ago/ 1999	BSD, Cisco, Nokia
2710		Descubrimiento de nodos multicast (MLD) para IPv6	Standards track	Oct/ 1999	Cisco, AT&T, IBM
2711		Opción alerta de router IPv6	Standards	Oct/	BBN

			track	1999	
2732		Formato para la representación literal de direcciones IPv6 en URL´s	Standards track	Dic/ 1999	Nokia, IBM, AT&T
2740		OSPF para IPv6	Standards track	Dic/ 1999	Siara, Juniper, Sicamore
2765		Algoritmo de Traslación Stateless IP/ICMP (SIIT)	Standards track	Feb/ 2000	Sun Microsystems
2766		Protocolo de Traslación - Traslación de Dirección de Red	Standards track	Feb/ 2000	BT, Campio Comm.
2767		Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)	Informativo	Feb/ 2000	Hitachi
2772	2546	Guias de ruteo en el troncal 6BONE	Informativo	Feb/ 2000	Sprint, ESnet
2776		Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)	Standards track	Feb/ 2000	ACIRI, Microsoft, Motorola
2874		Extensiones DNS para el soporte de agregación de dirección IPv6 y renumeración	Standards track	Jul/ 2000	Fermilab, Microsoft
2893	1933	Mecanismos de transición para hosts y routers IPv6	Standards track	Ago/ 2000	Freegate, SUN
2894		Renumeración de router para IPv6	Standards track	Ago/ 2000	Fermilab
2928		Asinación inicial de ID ´s subTLA IPv6	Informativo	Sep/ 2000	Nokia, Cisco, LBLN, Microsoft
3019		MIB IPv6 para el protocolo MLD	Standards track	Ene/ 2001	Nortel Networks, IBM
3041		Extensiones secretas para la autoconfiguración de direcciones stateless en IPv6	Standards track	Ene/ 2001	IBM, Microsoft
3056		Conexión de dominios IPv6 por la via de nubes IPv4	Standards track	Feb/ 2001	Carpenter, Moore
3122		Extensiones al descubrimiento de vecinos IPv6 para la especificación de descubrimiento inverso	Standards track	Jun/ 2001	Transwitch Corp.
3146		Transmisión de paquetes IPv6 sobre redes IEEE 1394	Standards track	Oct/ 2001	Sony Corp.
3177		Recomendaciones IAB/IESG sobre la asignación de direccion IPv6 a sitios.	Informativo	Sep/ 2001	IAB, IESG
3178		Soporte multihoming IPv6	Informativo	Oct/	Research laboratory

		en routers de salida de sitio		2001	IIJ, Vail Systems
3306		Direcciones multicast IPv6 basadas en el prefijo Unicast	Standards track	Ago/ 2002	Haberman consultant, Microsoft
3314		Recomendaciones para IPv6 en estandares del proyecto de asociaciones de tercera generación (3GPP)	Informativo	Sep/ 2002	M. Wasserman
3316		Protocolo de Internet versión 6 (IPv6) para algunos hosts celulares de segunda y tercera generación	Informativo	Abr/ 2003	Ericsson, Nokia
3484		Selección de la dirección por default para el protocolo de Internet versión 6 (IPv6)	Standards track	Feb/ 2003	Microsoft Research
3493	2553	Extensiones de la interfaz de socket basico para IPv6	Informativo	Feb/ 2003	Intransa, Cisco, H.P.
3513	2373	Arquitectura de direccionamiento del protocolo de Internet (IPv6)	Standards track	Abr/ 2003	Nokia, Cisco
3531		Método flexible para administrar la asignación de bits de un bloque de dirección IPv6	Informativo	Abr/ 2003	Viagenie
3542	2292	Sockets avanzados para la API IPv6	Informativo	May/ 2003	Sun, Toshiba
3574		Escenarios de transición para redes 3GPP	Informativo	Ago/ 2003	Nokia
3587	2374	Formato de la dirección Unicast global IPv6	Informativo	Ago/ 2003	Nokia, Cisco, Sun
3697		Especificación de la etiqueta de flujo IPv6	Standards track	Mar/ 2004	Nokia, Transwitch, IBM, Cisco
3701	2471	Asignación de direcciones de prueba IPv6 6BONE fase externa	Informativo	Mar/ 2004	Fink, Hinden
3769		Requerimientos para la delegación de prefijos IPv6	Informativo	Jun/ 2004	NTT Communi., Cisco
3775		Soporte de movilidad en IPv6	Standards track	Jun/ 2004	Rice Univer. Nokia, Ericsson
3776		IPSec para movilidad IPv6	Standards track	Jun/ 2004	Nokia, Ericsson
3879		Direcciones site local desaprobadas	Standards track	Sep/ 2004	Microsoft, IBM
3986	2732, 2396, 1808	Identificador de recursos uniforme (URI)	Standards track	Ene/ 2005	MIT, Day Software, Adobe systems
4007		Arquitectura de dirección de	Standards	Mar/	Cisco, Toshiba, SUN,

		ambito IPv6	track	2005	Microsoft
4022	2012 y 2452	Base de información de administración (MIB) para TCP IPv6	Standards track	Mar/ 2005	Cisco
4087	2667	MIB del túnel IP	Standards track	Jun/ 2005	Microsoft

APÉNDICE C

Glosario de Términos IPv6.

❖ **6over4**

6over4 es una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

❖ **6to4**

6to4 es una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

A

❖ **Agente**

Un servidor o un relay (ver definición de relay).

❖ **Agente propio**

El agente propio (home agent) es un router situado en el enlace propio que mantiene información sobre la localización de los nodos móviles que están fuera de la red propia y de la dirección temporal (care-of) que están empleando. Si el nodo móvil está en la red propia, el agente propio opera como un router tradicional. Si el nodo móvil está fuera de la misma el agente propio envía los datos al nodo a través de un túnel que establece hasta la dirección temporal (care-of) del mismo.

❖ **AH**

Protocolo de seguridad para la autenticación de cabecera (Authentication Header). Ver Cabecera de autenticación.

❖ **Alcanzabilidad**

Reachability determina si el envío en un sentido hacia un nodo funciona apropiadamente.

❖ **Ámbito (Scope)**

Para las direcciones IPv6, el ámbito es la porción de la red a la que se supone que se va a propagar el tráfico.

❖ **Anuncio de routers**

El anuncio de router (router advertising) es un mensaje de descubrimiento de vecinos (neighbor discovery) enviado por un router bien de forma pseudo-periódica o como respuesta a un mensaje de solicitud de router (router solicitation). El anuncio incluye al menos información acerca de un prefijo que será el que luego utilice el host para calcular su dirección IPv6 unicast según el mecanismo "stateless".

❖ **Arquitectura de pila dual**

La arquitectura de pila doble (dual stack) es una arquitectura para nodos IPv6/IPv4 en la que existen dos implementaciones completas de la pila de protocolos, una para IPv4 y otra para IPv6, cada una de ellas con su propia implementación de la capa de transporte (TCP y UDP).

❖ **Autoconfiguración de direcciones**

Es un proceso de configuración automática de direcciones IPv6 en una interfaz, puede ser de dos tipo autoconfiguración stateful y autoconfiguración stateless. Ver autoconfiguración de direcciones stateful y autoconfiguración de direcciones stateless.

❖ **Autoconfiguración de direcciones stateful**

La autoconfiguración de direcciones stateful utiliza un protocolo de autoconfiguración de direcciones "stateful", por ejemplo DHCPv6, para obtener direcciones IPv6 y parámetros de configuración asociados. Esta configuración requiere de la existencia de un servidor que proporcione los parámetros necesarios para la realización de la autoconfiguración o por lo menos las direcciones que se pueden usar.

❖ **Autoconfiguración de direcciones stateless**

La autoconfiguración stateless no requiere la existencia de algún servidor que proporcione por lo menos las direcciones, usa procedimientos de descubrimiento de vecinos (neighbor discovery) y anuncios de routers (router advertising) para obtener las direcciones IPv6 y los parámetros de configuración asociados.

B

❖ **Bucle de ruteo**

El bucle o lazo (loop) es una ruta donde los paquetes nunca alcanzan su destino, en lugar de ello, pasan por ciclos repetidamente a través de una serie constante de nodos de red. El bucle de ruteo es una situación indeseable en una red, que provoca que el tráfico se retransmita siguiendo un bucle cerrado, con lo cual el trafico nunca llega a su destino.

C

❖ **Cabecera de autenticación**

La cabecera de autenticación (autentication header) es una cabecera de extensión IPv6 que proporciona autenticación del origen de los datos, integridad de datos y servicio anti-repetición para la carga del datagrama y la cabecera IPv6 a excepción de los campos variables.

❖ **Cabeceras de extensión**

Las cabeceras de extensión (extensión headers) son las cabeceras que se sitúan entre la cabecera (header) del datagrama IPv6 y las cabeceras de los protocolos de nivel superior (TCP y UDP). Estas cabeceras son empleadas para dotar de funcionalidades adicionales a IPv6.

❖ **Cabecera de fragmentación**

La cabecera de fragmentación (fragmentation header) es una cabecera de extensión IPv6 que contiene información que es utilizada en el nodo receptor para reensamblar paquetes que tuvieron que ser divididos en paquetes más pequeños antes de su transmisión.

❖ **Cabecera de opción de salto-por-salto**

La cabecera de salto por salto (hop-by-hop) es una cabecera de extensión de IPv6 que contiene opciones que deben ser procesadas por todos los routers intermedios desde el origen hasta el final.

❖ **Cache**

Una pequeña área de memoria que contiene información almacenada en un nodo por un periodo de tiempo.

❖ **Cache de routers=caché de destinos**

La cache de routers o cache de destinos es una tabla mantenida por cada nodo IPv6, en esa tabla se mapea cada dirección (o rango de direcciones) destino con la dirección del siguiente router al que hay que enviar el datagrama. Además almacena la MTU de la ruta asociada.

❖ **Caché de vecinos**

La cache de vecinos es una tabla mantenida por cada nodo IPv6, la tabla almacena la dirección IP de sus vecinos en el enlace, sus correspondientes direcciones de nivel de enlace, y una indicación de su estado de accesibilidad. Las caché de vecinos es equivalente a la caché ARP en IPv4.

❖ **Capa IP doble**

La capa IP doble (dual) es una arquitectura para nodos IPv6/IPv4 en la que existe una única implementación de la capa de transporte como TCP o UDP que opera sobre implementaciones distintas de la capa de red IPv6/IPv4.

❖ **Care-of address**

Ver la definición de dirección care-of.

❖ **Checksum de la capa superior**

La suma de comprobación (checksum) es el cálculo del checksum realizado en ICMPv6, TCP y UDP que utiliza la pseudo-cabecera IPv6.

❖ **CNA**

Ver dirección del nodo corresponsal.

❖ **COA**

Dirección temporal (Care-of Address), ver dirección care-of.

❖ **Control de acceso al medio**

Es el subnivel mas bajo del nivel de enlace de datos ISO definido por el IEEE. Sus funciones son la creación de tramas y la gestión del acceso al medio.

❖ **Correspondencia del prefijo más largo**

Longest prefix match es el proceso de determinación de cual prefijo incluye una dirección IPv6. Cuando varios prefijos cubren una dirección el más largo es el que le corresponde.

❖ **Costo**

Métrica asociada con un enlace o una ruta.

D

❖ **Datagrama**

Sinónimo de paquete. Ver paquete.

❖ **Descubrimiento de prefijo**

El descubrimiento de vecinos es un procedimiento de descubrimiento de vecinos que permite a un determinado host o equipo final descubrir los prefijos de red para destinos de enlace local o de cara a los procedimientos de configuración de direcciones "stateless".

❖ **Descubrimiento de receptores multicast**

El descubrimiento de receptores multicast es un conjunto de mensajes ICMPv6 empleados por equipos y routers para gestionar los miembros de un grupo multicast en una subred.

❖ **Descubrimiento de la MTU de la ruta**

El descubrimiento de la unidad de transferencia máxima (MTU) transmite mensajes Too Big mediante ICMPv6 para descubrir el valor máximo de la MTU IPv6 en todos los enlaces entre dos equipos.

❖ **Descubrimiento de parámetros**

En el proceso de descubrimiento de vecinos que permite a los equipos se conocen los parámetros de configuración, incluyendo la MTU del enlace y el límite de saltos por defecto para los paquetes salientes.

❖ **Descubrimiento de routers**

El descubrimiento de routers (router discovery) es el procedimiento de descubrimiento de vecinos que permite descubrir los routers conectados en un determinado enlace.

❖ **Descubrimiento de vecinos**

El descubrimiento de vecinos (neighbor discovery) es un conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nodos vecinos. El descubrimiento de vecinos reemplaza a ARP, el descubrimiento de rutas ICMP y el mensaje de redirección ICMP empleados en IPv4. También proporciona detección de vecino inaccesible.

❖ **Detección de accesibilidad de vecinos**

Para determinar si un vecino es accesible se usa el proceso de descubrimiento de vecinos que determina si el nivel IPv6 de un vecino puede o no recibir paquetes. El estado de accesibilidad de cada vecino con el que se comunica un nodo se almacena en la caché de vecinos del mismo.

❖ **Descubrimiento de dirección del agente propio**

El descubrimiento del agente propio (home agent) es un proceso en el concepto de la movilidad IPv6 mediante el que un nodo móvil que está fuera de su red descubre la lista de agentes propios que están en su enlace propio.

❖ **Dirección**

La dirección es un identificador lógico asignado en el nivel de la capa de red IPv6 a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en el encabezado de los datagramas IPv6.

❖ **Dirección 6over4**

Una dirección 6over4 es una dirección del tipo [prefijo 64-bits]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4.

❖ **Dirección 6to4**

Una dirección 6to4 es una dirección del tipo 2002:WWXX:YYZZ:[SLA ID 16 bits]:[Interfaz ID 64 bits], en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica IPv4), empleada para representar un nodo en la tecnología 6to4.

❖ **Dirección anycast**

La dirección anycast es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un ruteo apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, el más cercano.

❖ **Dirección anycast de router de subred**

Es una dirección anycast con prefijo de 64 bits que se asigna a las interfaces de los routers.

❖ **Dirección care-of**

La dirección temporal (care-of), es una dirección global IPv6 utilizada por un nodo móvil cuando está conectado a un enlace ajeno. Se usa más el término inglés care-of address o CoA.

❖ **Dirección compatible con IPv4**

La dirección compatible con IPv4 (v4-compatible o compatibles-IPv4) es una dirección de la forma 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z, donde w.x.y.z es la representación decimal de una dirección pública IPv4. Por ejemplo, ::192.0.0.182 es una dirección compatible con IPv4. Estas direcciones se emplean en túneles IPv6 Automáticos.

❖ **Dirección de capa de enlace**

Es la dirección de capa 2 del modelo OSI de una interfase.

❖ **Direcciones de compatibilidad**

Las direcciones de compatibilidad son las direcciones IPv6 que son empleadas al enviar tráfico IPv6 sobre una infraestructura IPv4. Ejemplos de direcciones de compatibilidad son: las direcciones compatibles-IPv4 (::w.x.y.x), las direcciones 6to4 (2002:wwxx:yyzz:[SLAID]:[InterfazID]) y las direcciones ISATAP (FE80::5EFE:w.x.y.z).

❖ **Dirección de lazo local**

La dirección de lazo local (loopback) es una dirección IPv6 especial ::1, que se asigna a la interfaz local, las pruebas a esta dirección nunca salen del equipo, se hacen internamente a la interfaz local.

❖ Dirección desaprobada

Deprecated address. Es la dirección asociada con una interfaz cuyo uso por parte de los protocolos superiores esta desalentada.

❖ **Dirección de uso local**

La dirección de uso (ámbito) local es una dirección unicast IPv6 que no es alcanzable en la Internet IPv6. Las direcciones de uso local incluyen las direcciones locales del enlace (link local FE80::/10) y las direcciones locales del sitio (site local FEC0::/10).

❖ **Dirección del agente propio**

La dirección del agente propio (home agent) es la dirección global IPv6 de la interfaz del agente propio situado en el enlace propio en la arquitectura de movilidad IPv6.

❖ **Dirección del nodo corresponsal**

La dirección del nodo corresponsal es la dirección global asignada a un nodo corresponsal cuando se comunica con un nodo móvil que se encuentra fuera de su red propia.

❖ **Dirección EUI-64**

La dirección del identificador universal extendido EUI-64 (Extended Universal Identifier) es una dirección del nivel de enlace de 64 bits que se usa como base para la generación de identificadores de interfaz en IPv6 a partir de la dirección física o MAC del nodo..

❖ **Dirección global**

Global Address. Una dirección mundialmente única.

❖ **Dirección global de agregación unicast o dirección global**

Las direcciones globales de agregación unicast (unicast aggregatable global) también conocidas como direcciones globales, las direcciones globales agregables unicast se identifican por el formato del prefijo 001 (2000::/3). Las direcciones globales IPv6 son equivalentes a las direcciones públicas IPv4 y son globalmente ruteables y alcanzables en la Internet IPv6.

❖ **Dirección invalida**

Es una dirección no asignada a ninguna interfaz.

❖ **Dirección IPv4 mapeada**

La dirección mapeada a IPv4 es una dirección de la forma 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, donde w.x.y.z es una dirección IPv4. Las direcciones IPv4 mapeadas se emplean para representar un nodo con soporte sólo IPv4 ante un nodo IPv6.

❖ **Dirección ISATAP**

La dirección de protocolo de túnel automático intrasite ISATAP (IntraSite Automatic Tunneling Protocol) es una dirección del tipo [prefijo de 64-bit]:0:5EFE:w.x.y.z, siendo w.x.y.z una dirección IPv4, pública o privada, que se asigna a un equipo ISATAP.

❖ **Dirección local de sitio**

La dirección de uso (ámbito) local al sitio, es una dirección de uso local identificada por el prefijo de diez bits de longitud 1111 1110 11 (FEC0::/10). El ámbito de utilización de ese tipo de direcciones es el "sitio" local (de una organización), sin la necesidad de un prefijo global. Las direcciones locales de sitio no son accesibles desde otros sitios y los routers no deberían encaminar tráfico correspondiente al sitio local fuera del propio sitio. En la actualidad, se debate la necesidad de las mismas, y muy probablemente desaparezcan de la especificación de IPv6.

❖ **Dirección local del enlace**

La dirección de uso (ámbito) local al enlace es una dirección de uso local identificada por el prefijo de diez bits de longitud 1111 1110 10 (FE80::/10), cuyo ámbito es el del enlace local. Los nodos utilizan estas direcciones para comunicarse con nodos vecinos en el mismo enlace. Son equivalentes a direcciones privadas IPv4 APIPA (Automatic Private IP Addressing).

❖ **Dirección MAC**

La dirección de control de acceso al medio MAC (Medium Access Control) es una dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se le conoce como dirección física, dirección del hardware o dirección del adaptador de red.

❖ **Dirección multicast**

La dirección multicast identifica múltiples interfaces y se emplea en entregas de datos uno-a-muchos. Mediante una topología de ruteo multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

❖ **Dirección no especificada**

La dirección no especificada es una dirección IPv6 especial de la forma 0:0:0:0:0:0:0:0 (::) que se emplea para reflejar la ausencia de una dirección, de forma equivalente a la dirección 0.0.0.0 de IPv4.

❖ **Dirección preferida**

Preferred Address. Es la dirección asociada con una interfaz cuyo uso por parte de los protocolos superiores es permitido sin limitación.

❖ **Dirección propia**

La dirección propia (home address) es una dirección global IPv6 asignada al nodo móvil cuando está unido al enlace local y a través del cual el nodo es alcanzable independientemente de su localización en la Internet IPv6.

❖ **Dirección temporal o dirección anónima**

La dirección temporal es una dirección que utiliza un identificador de interfaz obtenida aleatoriamente. Este tipo de direcciones cambia con el tiempo, dificultando el seguimiento de las actividades de un host IPv6.

❖ **Dirección tentativa**

Es una dirección unicast cuya unicidad no se ha comprobado todavía y debe ser verificada dentro de un enlace antes de asignarla a una interfaz.

❖ **Dirección unicast**

Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquél en el que esa dirección es única.

❖ **Dirección valida**

Una dirección preferida o desaprobada

❖ **DNS**

Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones. Ver sistema de nombres de dominio (Domain Name System.)

❖ **Dominio de ruteo**

Routing Domain. Particionamiento jerárquico de la red que contiene hosts y routers. Los routers comparten la misma información de ruteo, calculan las tablas usando el mismo IGP y son administrados por una autoridad común.

❖ **Dos puntos dobles (double colon)**

El símbolo dos puntos dobles (double colon) representado como :: es la forma práctica de comprimir series continuas de bloques de 0 en las direcciones IPv6. Por ejemplo, la dirección de multicast FF02:0:0:0:0:0:0:2 se expresa como FF02::2. Si hay dos series de bloques de 0, de longitud máxima, sólo se codifica de esta manera el bloque que figura más a la izquierda de la dirección.

❖ **DHCP**

El protocolo de configuración de hosts dinámico DCHP (Dynamic Host Configuration Protocol) es un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP en presencia de un servidor implementado para ello.

E

❖ **ESP**

El encabezado de seguridad de la carga útil o datos ESP (Encapsulating Security Payload) e una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga útil del datagrama encapsulado por la cabecera y cola.

❖ **Enlace**

Uno o más segmentos de una red de área local limitados por routers forman un enlace. Una instalación o medio de comunicación sobre el cual, los nodos se comunican en la capa de enlace de datos o capa 2 del modelo OSI/ISO. Ejemplos de enlaces son Ethernet, X.25, Frame Relay, PPP y ATM, o túneles sobre otros protocolos como IPv4 o IPv6.

❖ Estado de enlace

Link state. Algoritmo de ruteo que calcula las tablas de ruteo con el cual un router comunica a los otros el estado de los enlaces directamente conectados a el, a través de un paquete de estado de enlace.

❖ **NBMA**

El enlace de acceso múltiple sin broadcast NBMA (Non-Broadcast Múltiple Access) es una tecnología de nivel de enlace que soporta enlaces con más de dos nodos, pero sin permitir el envío de un paquete a múltiples destinos (broadcast). Por ejemplo, X.25, Frame Relay y ATM.

❖ **Enlace propio**

En un ambiente de movilidad IP el enlace propio (home link), es el enlace en el que el nodo móvil reside en su red. El nodo móvil, emplea el prefijo del enlace propio para crear su dirección propia (home address).

❖ **Estado de enlace**

El algoritmo de estado de enlace (link state) es usado en las tecnologías de protocolos de ruteo, esta tecnología intercambia información de rutas que consta de los prefijos de las redes conectadas a un router y su costo asociado. La información del estado del enlace se anuncia en el arranque, así como cuando se detectan cambios en la topología de la red.

❖ **EUI**

El identificador único extendido EUI (Extended Unique Identifier) es una dirección del nivel de enlace definida por el IEEE (Institute of Electrical and Electronic Engineers).

F

❖ **Fichero hosts**

El archivo hosts es un fichero de texto empleado para contener correspondencias nombre-dirección IP. En windows XP o .NET server está en el directorio \SystemRoot\System32\Drivers\Etc. En máquinas Unix está en el directorio /etc. En algunos sistemas también se conoce como lmhosts.

❖ **Flujo**

Un flujo se define como una serie de datagramas (pertenecientes al mismo tipo de información) intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto de 0.

❖ **Fragmentación**

La fragmentación es el proceso con el que se divide la carga útil de un datagrama IPv6 en fragmentos por la máquina emisora de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

❖ **Fragmento**

Una porción de una carga en un datagrama IPv6 enviada por un host. Los fragmentos contienen una cabecera de fragmentación.

G

❖ **Grupo de máquinas (host group)**

Es un conjunto de máquinas que en tráfico multicast escuchan una determinada dirección multicast.

❖ **Grupo multicast**

Conjunto de equipos escuchando una dirección multicast específica.

H

❖ **HA**

Dirección propia (Home Address), ver dirección propia.

❖ **HAA**

Dirección del agente propio (Home Agent Address), ver dirección del agente propio.

❖ **Home agent**

Ver agente propio.

❖ **Home agent address discovery**

Ver descubrimiento de dirección del agente propio.

❖ **Home link**

Ver enlace propio.

❖ **Host**

Cualquier nodo que no es un router. Ver máquina (host).

I

❖ **ICMPV6**

El protocolo de mensajes para el control de Internet en IPv6 ICMPv6 (Internet Control Message Protocol) es un protocolo que proporciona mensajes de error para el ruteo y entrega de datagramas IPv6 y mensajes de información para diagnóstico, descubrimiento de vecinos, descubrimiento de receptores multicast y movilidad IPv6.

❖ **Identificador de agregación de sitio**

El identificador de agregación de sitio SLA ID (Site-Level Aggregation Identifier) es un campo de 16 bits dentro de la dirección global unicast que utiliza una organización para identificar subredes dentro de su red.

❖ **Identificador de agregación de máximo nivel**

El identificador de agregación de máximo nivel TLA ID (Top-Level Aggregation Identifier), es un campo de 13 bits dentro de la dirección unicast global reservado para grandes organizaciones o ISPs por el IANA, este campo identifica el rango de direcciones que tienen delegado.

❖ **Identificador de agregación de siguiente nivel**

El identificador de agregación de siguiente nivel NLA ID (Next-Level Aggregation Identifier) es un campo de 24 bits en la dirección unicast global agregable que permite a los ISPs crear varios niveles jerárquicos de direccionamiento en sus redes para organizar las direcciones y el ruteo hacia otros ISPs, así como para identificar los sitios de la organización.

❖ **Identificador de grupo**

El identificador de grupo se forma de los últimos 112 bits o los últimos 32 bits (de acuerdo a la recomendación de la RFC 2373) de una dirección IPv6 multicast, que identifica un grupo de multicast.

❖ **Identificador de interfaz**

El identificador de interfaz son los últimos 64 bits de una dirección IPv6 unicast o anycast.

❖ **Interfaz**

La interfaz es la representación de una conexión física o lógica de un nodo a un enlace. Una interfaz física es por ejemplo un interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de túnel.

❖ **Interfaz local**

La interfaz local es la interfaz interna que permite que un nodo se envíe paquetes a sí mismo usando direcciones de loopback.

❖ **Intranet**

Red privada basada en el modelo de Internet.

❖ **IPV6 en IPV4**

Ver túneles IPv6 sobre IPv4.

❖ **IP6.INT**

Los registros IP6.INT forman el dominio DNS creado para la resolución inversa en IPv6. La resolución inversa tiene por objeto determinar el nombre de una máquina a partir de su dirección.

❖ **IPSEC**

La seguridad del protocolo de Internet IPSEC (Internet Protocol Security) es un marco de estándares abiertos que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPSEC soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección ante repeticiones.

❖ **ISATAP**

Ver protocolo de direccionamiento de túneles internos automáticos ISATAP (Intrasite Automatic Tunneling Addressing).

J

❖ **Jumbograma**

El datagrama gigante o jumbograma es un paquete IPv6 que tiene una carga útil mayor de 65.535 bytes. Los jumbogramas se indican con un valor 0 en el campo de longitud de carga útil de la cabecera IPv6, e incluyendo una opción de carga útil del Jumbo en la cabecera de opciones Salto-a-Salto.

L

❖ **Lista de agentes propios**

La lista de agentes propios (home agent) son una tabla mantenida por los agentes propios en la que se almacena la lista de routers en el enlace propio (link agent) que pueden actuar como agentes propios.

❖ **Lista de prefijos**

Es la lista de prefijos de enlace mantenida por cada host. Cada entrada define directamente el rango de direcciones IP que son alcanzables directamente, es decir, los vecinos.

❖ **Lista de routers de defecto**

Esta también es una lista mantenida por cada máquina, en la que aparecen todos los routers de los que se ha recibido un anuncio de router con un valor de "Tiempo de vida de router" no nulo.

LL

❖ **Llamada a procedimientos remotos**

La llamada a procedimientos remotos RPC (Remote Procedure Call), es una interfaz utilizada para crear programas cliente/servidor distribuidos. Las librerías que implementan el sistema de llamadas a procedimientos remotos o RPCs se encargan de gestionar los detalles relacionados con los protocolos de red y las comunicaciones.

M

❖ **MAC**

Control de acceso al medio MAC (Médium Access Control), ver control de acceso al medio, dirección MAC.

❖ **Máquina (Host)**

Una maquina o host es un nodo que no puede reenviar datagramas no originados por sí mismo. Una máquina es típicamente el origen y destino del tráfico IPv6 y va a descartar discretamente tráfico que no esté dirigido específicamente a él mismo.

❖ **Máquina 6to4**

Una máquina 6to4 es un host IPv6 que está configurado con al menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Las máquinas 6to4 no requieren configuración manual y crean las direcciones 6to4 empleando mecanismos clásicos de autoconfiguración.

❖ **Máquina ISATAP**

Una maquina ISATAP (Intra Site Automatic Tunneling Addressing Protocol) es un equipo al que se le asigna una dirección ISATAP.

❖ **MLD**

Multicas Listening Discovery. Ver descubrimiento de receptores Multicast.

❖ **Movilidad IPv6**

La movilidad IPv6 (Mobile IPv6) es un conjunto de mensajes y procesos que permiten a un nodo IPv6 cambiar arbitrariamente su posición (subred de acceso a Internet IPv6) y mantener activas las conexiones establecidas previamente.

❖ **MTU**

La unidad de transmisión máxima MTU (Maximum Transmission Unit) es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

❖ **MTU del enlace**

La unidad máxima de transmisión (MTU) del enlace es el tamaño del paquete IPv6 máximo en octetos (bytes) que puede enviarse sobre el enlace sin fragmentación. Dado que el tamaño máximo de trama incluye las cabeceras y colas de nivel de enlace, la MTU del enlace no coincide con el tamaño máximo de trama del enlace. La MTU del enlace coincide con el máximo tamaño de carga útil de la tecnología de nivel de enlace.

❖ **MTU de la ruta**

La unidad de transmisión máxima de la ruta (Path MTU) es el tamaño máximo de un paquete IPv6 que puede enviarse sin emplear fragmentación entre una fuente y un destino sobre una ruta en una red IPv6. La MTU de la ruta coincide con la menor MTU de todos los enlaces entre un nodo fuente y un nodo destino.

❖ **MTU IPv6**

El tamaño máximo de un paquete IP que se puede enviar sobre un enlace.

❖ **Multihomed**

Red perteneciente a dos o más dominios de ruteo.

N

❖ **NAT**

El traductor de direcciones de red NAT (Network Address Translation) Es un router IPv4 que traduce direcciones y puertos al reenviar paquetes entre una red con direcciones privadas e Internet.

❖ **ND**

Descubrimiento de vecinos (Neighbor Discovery). Ver descubrimiento de vecinos.

❖ **NLA ID**

Identificador de agregación de siguiente nivel NLA ID (Next Level Aggregation Identifier). Ver identificador de agregación de siguiente nivel.

❖ **Nodo corresponsal**

Un nodo corresponsal es un nodo que se comunica con un nodo móvil que se encuentra fuera de su red propia..

❖ **Nodo IPv4**

Es un nodo que implementa IPv4; puede enviar y recibir paquetes IPv4. Puede ser un nodo con soporte sólo IPv4 o un nodo dual IPv4/IPv6.

❖ **Nodo IPv6**

Es nodo que implementa IPv6 (Puede enviar y recibir paquetes IPv6). Un nodo IPv6 puede ser bien un nodo con soporte IPv6 o un nodo dual IPv6/IPv4.

❖ **Nodo IPv6/IPv4**

Es un nodo que dispone de implementaciones de IPv4 e IPv6.

❖ **Nodo móvil**

Es un nodo IPv6 que puede cambiar el punto de acceso a Internet IPv6 y por tanto su dirección, y mantener también su alcanzabilidad a través de su dirección propia. Un nodo móvil conoce tanto su dirección propia (home address) como su dirección temporal (care-of) y comunica este mapeado tanto al agente propio (home agent) como a los nodos corresponsales con los que tiene una comunicación establecida.

❖ **Nombre ISATAP**

Es el nombre resuelto por ordenadores con sistema operativo Windows XP Service Pack 1 o bien de la familia de Windows .NET Server 2003 para descubrir automáticamente la dirección del router ISATAP. Los equipos con Windows XP tratan de resolver el nombre "_ISATAP."

❖ **Notación hexadecimal separada con dos puntos**

La notación hexadecimal separada con dos puntos (colon hexadecimal notation) es la notación empleada para expresar direcciones IPv6. La dirección de 128 bits es dividida en 8 bloques de 16 bits. Cada bloque se expresa como un número hexadecimal y éstos se separan del siguiente por medio del signo ortográfico dos puntos (:). Dentro de cada bloque, los ceros situados a la izquierda son eliminados. Un ejemplo de una dirección IPv6 unicast representada en notación hexadecimal separada por dos puntos es 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

❖ **Notación prefijo-longitud**

La notación prefijo-longitud o prefijo/longitud es la notación mediante la cual se expresan los prefijos de red. Tiene la forma dirección/longitud del prefijo, siendo dicha longitud el número de bits iniciales de la dirección que se fijan para definir el prefijo.

❖ **NUD**

Ver detección de accesibilidad de vecinos.

O

❖ **Obtención del salto siguiente**

Es el proceso de obtención de la dirección o interfaz del siguiente salto para enviar o reenviar un paquete basándose en el contenido de la tabla de ruteo.

❖ **Off-link**

Una dirección IPv6 que no esta asignada a ninguna interfaz sobre el enlace especifico.

❖ **On-link**

Una dirección IPv6 que esta asignada a una interfaz sobre un enlace especifico

❖ **Opción de carga útil del jumbo**

Una opción en la cabecera de opciones Salto-a-Salto que indica el tamaño de un paquete gigante o jumbograma.

❖ **Opciones de descubrimiento de vecinos**

Son las opciones de los mensajes de descubrimiento de vecinos que indican las direcciones de nivel de enlace, información sobre los prefijos, MTU, redirecciones, rutas e información de configuración para movilidad IPv6.

P

❖ **Paquete**

Un paquete es la unidad de datos del protocolo (PDU) existente a nivel Internet IPv6. En el caso de IPv6, un paquete consta de una cabecera y la carga útil IPv6.

❖ **PDU**

Ver unidad de datos de protocolo (PDU).

❖ **Prefijo**

Es la parte inicial de una dirección IPv6 común a todos los nodos conectados al mismo enlace.

❖ **Prefijo de formato**

El prefijo de formato FP (format prefix) son los bits de mayor orden con un valor fijo que definen un tipo de dirección IPv6.

❖ **Prefijo de red**

Es la parte fija de la dirección que se utiliza para determinar el identificador de la subred, la ruta o el rango de direcciones.

❖ **Prefijo de sitio**

El prefijo de sitio normalmente es un prefijo de 48 bits que se utiliza para referirse a todas las direcciones del sitio. Los prefijos de sitio se almacenan en una tabla de prefijos que se emplea para confinar todo el tráfico asociado a esos prefijos dentro del sitio.

❖ **Protocolo de direccionamiento de túneles internos automáticos**

El protocolo de direccionamiento de túneles internos automáticos ISATAP (Intra Site Automatic Tunneling Addressing Protocol) es una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

❖ **Protocolo del nivel superior**

Es el protocolo que utiliza IPv6 como transporte y se sitúa en la capa inmediatamente superior a IPv6, como ICMPv6, TCP y UDP.

❖ **Protocolo punto-a-punto**

El protocolo punto a punto PPP (Point to Point Protocol) es un método de encapsulación de red punto-a-punto que proporciona delimitadores de tramas, identificación del protocolo y servicios de integridad a nivel de bit.

❖ **Protocolos de ruteo**

Los protocolos de ruteo son los procedimientos y conjuntos de mensajes relativos a rutas que se intercambian entre routers para construir las tablas de ruteo dinámicamente.

❖ **Protocolo de ruteo interior**

Interior Gateway Protocol (IGP). Termino genérico para los protocolos que anuncian alcanzabilidad e información de ruteo dentro de un sistema autónomo.

❖ **Protocolo de ruteo exterior**

Exterior Gateway Protocol (EGP). Termino genérico para los protocolos que anuncian alcanzabilidad e información de ruteo entre sistemas autónomos diferentes.

❖ **Proveedor de Servicios de Internet**

Internet Service Provider. Organización publica o privada que proporciona servicios de Internet, mas comúnmente conocida como proveedor.

❖ **Proxy**

Un router que responde a mensajes de consulta para el descubrimiento de vecinos ND en nombre de otro nodo como en el caso de nodos moviles.

❖ **Pseudo-cabecera**

Es una cabecera temporal que se construye para calcular el checksum necesario para asociar la cabecera IPv6 con la carga. En IPv6 se utiliza un nuevo formato de pseudo-cabecera al calcular el checksum de UPD, TCP e ICMPv6.

❖ **Pseudo-periódico**

Es un suceso que se repite en intervalos no constantes. Por ejemplo, el anuncio de rutas enviado por un router IPv6 se produce en intervalos que se calculan aleatoriamente entre un mínimo y un máximo.

R

❖ **Red**

Una red son dos o más subredes conectadas por routers. Otro término empleado es interred.

❖ **Redireccionar**

Procedimiento englobado dentro de los mecanismos de descubrimiento de vecinos por el cual se informa a un host de la dirección IPv6 de otro que resulta más adecuado como siguiente salto hacia un determinado destino.

❖ **Reensamblado**

El reensamblado es el proceso mediante el cual se reconstruye la carga original de un datagrama a partir de varios fragmentos.

❖ **Registro de direcciones de equipos IPv6**

Ver registro AAAA.

❖ **Registro AAAA**

El registro de direcciones de equipos IPv6 AAAA es el tipo de registro en el DNS (Sistema de Nombres de Dominio) que se emplea para resolver un nombre FDQN (Fully Qualified Domain Name) a una dirección IPv6.

❖ **Registro PTR**

Es un registro de DNS que permite resolver una dirección IP a un nombre.

❖ **Relay**

Un nodo que actúa como un dispositivo intermediario en la transmisión de un paquete entre otros dos nodos (entre un cliente y servidor).

❖ **Resolución de nombres**

Es el proceso de obtención de una dirección a partir de un nombre. En IPv6, la resolución de nombres permite obtener direcciones a partir de nombres de equipos o nombres de dominio totalmente calificados (FQDN).

❖ **Retardo de unión**

Tiempo transcurrido entre el envío de un mensaje de informe de escucha de multicast (Multicast Listener Report) por parte de un nuevo miembro de un grupo multicast en una subred que no dispone de miembros de grupo, y el envío de los paquetes multicast de ese grupo sobre la subred.

❖ **Resolución de direcciones**

Es el proceso de resolución de direcciones del nivel de enlace para la dirección de next-hop (siguiente salto, gateway) en un enlace. En una red de área local (LAN) conectada a Internet, el proceso automático mediante el cual la dirección de LAN de cada estación de trabajo se convierte en una dirección IP.

❖ **Router**

Es un nodo que puede retransmitir datagramas que no van específicamente destinados a él. En una red IPv6 un router suele enviar además anuncios relativos a su presencia y su información de configuración. A veces denominado enrutador o encaminador.

❖ **Router advertisement**

Ver anuncio de routers.

❖ **Router exterior**

Exterior router. Router que maneja las conexiones entre diferentes sistemas autónomos.

❖ **Router interior**

Interior router. Router que maneja las conexiones solamente dentro de un AS.

❖ **Router relay 6to4**

Un router relay 6to4 es un router IPv6/IPv4 que redirige tráfico dirigido a direcciones 6to4 entre routers 6to4 en Internet y máquinas de la Internet IPv6

❖ **Router 6to4**

Es un router IPv6/IPv4 que soporta el empleo de un interfaz de túnel 6to4 empleado para reenviar tráfico dirigido a direcciones 6to4 entre máquinas 6to4 de una red y otros routers 6to4 o routers relay 6to4 en la Internet IPv4.

❖ **Router ISATAP**

Es un router IPv6/IPv4 que responde a las solicitudes de equipos ISATAP a través de túneles y encamina el tráfico entre equipos y nodos ISATAP de otra red o subred ISATAP.

❖ **Routing**

Determinación de la ruta que un paquete IP debe seguir para alcanzar su destino.

❖ **RPC**

Remote procedure call. Ver llamada a procedimientos remotos.

❖ **Ruta**

Path. Conjunto ordenado de enlaces que conectan una fuente con un destino.

❖ **Ruta asociada a una subred**

Es una ruta cuyo prefijo de 64 bits corresponde al de una subred en concreto.

❖ **Ruteo dinámico**

Dynamic routing. Técnica que calcula y actualiza las tablas de ruteo dinámicamente en base a la topología y estado de la red.

❖ **Ruta estática**

Entrada en la tabla de ruteo escrita manualmente por el administrador de la red.

❖ **Ruteo estático**

Static routing. El ruteo estático es la utilización de rutas introducidas manualmente en las tablas de ruteo de los routers durante la configuración de la red.

❖ **Ruta por defecto**

Es la ruta con prefijo ::/0. La ruta por defecto, recoge todos los destinos y es la ruta empleada para obtener la siguiente dirección de destino cuando no hay otras rutas coincidentes.

S

❖ **Salto**

Hop. El cruce de un enlace.

❖ **Segmento de una red de área local**

Es la porción de un enlace que consta de un único medio limitado por puentes o conmutadores (switches) de nivel 2.

❖ **Segmento de red**

Ver subred

❖ **Selección de ruta adecuada**

Es el algoritmo empleado por el proceso de selección de rutas para escoger las rutas de la tabla de ruteo que más se acercan a la dirección destino a la que se debe enviar o encaminar el paquete.

❖ **Siguiente salto**.

Next hop es el siguiente nodo hacia el cual se transmite el paquete. El nodo debe estar dentro del enlace y por lo tanto ser un vecino.

❖ **Sistema Autónomo**

Autonomous system (AS). Una porción de la red o conjunto de dominios de ruteo perteneciente a la misma autoridad administrativa.

❖ **Sistema de determinación de ruta**

Es el proceso por el cuál se selecciona cuál es la ruta concreta de la tabla de ruteo por la que se va a encaminar el datagrama. Esto es, se selecciona el siguiente router al que se va a mandar el datagrama.

❖ **Sistema de nombres de dominio**

Es un sistema jerárquico de almacenamiento y su protocolo asociado para almacenar y recuperar información sobre nombres y direcciones IP.

❖ **SLA ID**

Site Level Aggregation Identifier. Ver identificador de agregación de sitio.

❖ **Solicited-node address**

La dirección de nodo solicitada es una dirección muticast utilizada por los nodos durante el proceso de resolución de direcciones. La dirección de nodo solicitada se construye con el prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 unicast. Esa dirección se emplea a modo de pseudo dirección unicast para llevar a cabo una resolución de direcciones más eficiente en los enlaces IPv6.

❖ **Subred**

En IPv6 una subred es uno o más enlaces que utilizan el mismo prefijo de 64 bits. Conjunto de nodos identificados por direcciones con un prefijo común, estos nodos están conectados al mismo enlace.

T

- **Tabla de ruteo IPv6**

Es el conjunto de rutas empleadas para determinar la dirección e interfaz del siguiente nodo en el tráfico IPv6 enviado por un equipo o reencaminado por un router.

- **Target**

Una dirección buscada a través de un proceso de resolución o la dirección del primer salto obtenida a través del proceso de redireccionamiento.

- **Tiempo de vida en estado "preferred" preferida**

Es el tiempo durante el que una dirección unicast obtenida mediante el mecanismo de autoconfiguración stateless permanece en estado "preferred" o de preferida, antes de que se convierta en desaprobada. Este tiempo viene indicado por el campo "Preferred Lifetime" de la opción "Prefix Information" (información de prefijo) de los mensajes de anuncio de routers.

- **Tiempo máximo de validez de una dirección**

Tiempo en el que una dirección unicast conseguida mediante el proceso de autoconfiguración stateless permanece en estado válido (tanto preferido como desaprobado o deprecated).

- **TLA ID**

Top Level Aggregation Identifier. Ver identificador de agregación de máximo nivel.

- **Traductor de direcciones de red**

El traductor de direcciones de red NAT es un router IPv4 que traduce direcciones y puertos al reenviar paquetes entre una red con direcciones privadas e Internet.

- **Transición**

La transición usada en IPv6, consiste en la conversión de nodos sólo IPv4 a nodos con doble pila, o sólo IPv6.

- **Túnel**

Es un túnel IPv6 sobre IPv4, en los que los puntos finales son determinados por configuración manual.

- **Túnel automático**

Un túnel IPv6 sobre IPv4 en el que los puntos finales son determinados por el empleo de interfaces lógicas de túneles, rutas y direcciones orígenes y destino IPv6.

- **Túneles IPv6 automáticos**

Son túneles de creación automática que se emplean con direcciones compatibles con IPv4.

- **Túneles IPv6 sobre IPv4**

Consisten en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

- **Túnel IPv4 multicast**

Ver 6over4.

- **Túnel máquina-a-máquina**

Es un proceso de creación de túnel IPv6 sobre IPv4 en el que los dos extremos son máquinas.

- **Túnel máquina-a-router**

Es proceso de creación de túnel IPv6 sobre IPv4 en el que el túnel empieza en un host y acaba en un router IPv6/IPv4.

U

- **Unidad de datos del protocolo**

La unidad de datos de protocolo PDU (Protocolo Data Unit) es el conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

- **Unidad máxima de transmisión**

La unidad máxima de transmisión MTU (Maximum Transmission Unit) es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

- **Upper layer**

Una capa de protocolos inmediatamente arriba de IPv6, como los protocolos de transporte (TCP, UDP), protocolos de control (ICMP), protocolos de ruteo (RIP, OSPF), o protocolos de capa inferior que son tunelizados sobre IPv6.

V

- **Vecino**

Un nodo vecino (neighbor) es un nodo conectado al mismo enlace.

- **Vector de distancia**

Distance vector. Es un algoritmo de ruteo para protocolos de ruteo que calcula las tablas de ruteo en base al intercambio de tablas de ruteo entre nodos adyacentes y propaga información de ruteo en la forma de un identificador de red y su distancia en número de saltos.

- **Vector de ruta**

Es una tecnología de protocolo de ruteo que intercambia secuencias de información de saltos indicando el camino a seguir en una ruta. Por ejemplo, BGP-4 intercambia secuencias de números de sistemas autónomos.

Glosario de términos varios de telecomunicaciones.

A

- **A/D converter**

El convertidor analógico/digital A/D o ADC (Analog to Digital Converter) es un dispositivo que convierte señales analógicas continuas de instrumentos que supervisan condiciones como movimiento, temperatura, sonido, etc., en codigos binarios para una computadora.

- **AAL Adaption layer**

Capa de adaptación ATM AAL (Adaption Layer) es la colección de protocolos estándar que adapta el trafico de usuario a un formato de celdas de tamaño fijo. Esta capa se subdivide en la subcapa de convergencia (CS) y la subcapa de segmentación y reensamblado (SAR).

❖ **AAL tipo1**

Es el protocolo estándar usado para el transporte de tráfico de velocidad de bits constante CBR (Constant Bit Rate) como audio y video y para la emulación de circuitos basados en TDM (por ejemplo E1, T1).

❖ **AAL tipo 2**

Es el protocolo estándar que soporta el servicio de velocidad de bits variable VBR (Variable Bit Rate) dependiente del tiempo (VBR-RT) de tráfico orientado a conexión como audio y video paquetizado).

❖ **Abilene**

Es el nombre de una de las principales infraestructuras de red del proyecto Internet2

❖ **ABM**

Modo asíncrono balanceado (Asynchronous Balanced Mode).

❖ **Accesos conmutados**

Circuitos de acceso que se encuentran intercomunicados para mayor flujo de datos a la red.

❖ **ACL**

El control de acceso de una red es un medio de proteger la seguridad del sistema exigiendo a los usuarios que suministren un nombre de inicio de sesión y una contraseña.

Lista de control de acceso

La lista de control de acceso ACL (Access Control List) de una red es la base de datos que enlista los usuarios autorizados de los sistemas y el nivel de acceso a la red que se les ha otorgado.

❖ **Access method**

El método de acceso (access method) es una rutina del software, parte del sistema operativo o del programa controlador de la red, que realiza grabación y recuperación, o transmisión y recepción de datos. Responsable, también, de la detección de una mala transferencia de datos, causada por el mal funcionamiento del hardware o de la red.

❖ **ACK**

Respuesta afirmativa ACK (Affirmative Acknowledgement), en comunicaciones es el código enviado desde una estación de recepción a una de transmisión para avisar que está lista para aceptar datos. Es usado también para indicar que se recibieron los datos transmitidos sin errores.

❖ **Acknowledgement**

Acuse de recibo (Acknowledgement) es un tipo de mensaje que se envía para indicar que un bloque de datos ha llegado a su destino sin errores. Un acuse de recibo puede también ser negativo (no acknowledgement -- NOACK), es decir, indicar que un bloque de datos no ha llegado a su destino.

❖ **ACS**

Servidor de comunicaciones asíncronas (Asynchronous Communicatios Server) Servidor de comunicaciones que maneja un lote de modems. Dirige cada mensaje de salida al próximo modem disponible y dirige cada mensaje recibido a la estación de trabajo correspondiente.

❖ **Active star**

La estrella activa es una topología de red que proporciona la regeneración de señales en el núcleo central.

❖ **Actualización del horizonte dividido.**

Técnica de enrutamiento en la cual se evita que la información acerca de las rutas salga de la interfaz del ruteador a través del cual se recibió dicha información. Las actualizaciones del horizonte dividido son útiles para evitar los bucles de enrutamiento.

❖ **ADCCP**

Protocolo de control avanzado de comunicación de datos ADCCP (Advanced Data Communications Control Protocol). Procedimiento avanzado de control de comunicaciones de datos (Advanced Data Communications Control Procedure). Es un protocolo de comunicaciones ANSI, similar a los protocolos SDLC y HDLC.

❖ **Address Mask**

Mascara de dirección.

❖ **Address**

Dirección. En Internet una dirección es la serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: "dirección de correo electrónico" (email address); "IP" (dirección internet); y "dirección hardware" o "dirección MAC" (hardware or MAC address).

❖ **ADPCM**

Modulación diferencial adaptiva por codificación de pulsos (Adaptive Differential Pulse Code Modulation).

❖ **Analog**

Analógico hace referencia a valores o voltajes que varían continuamente en un rango infinito.

❖ **Analog modem**

Módem analógico es el tipo más común de módem. Los módems están diseñados para comunicarse a través de líneas de servicio telefónico convencional (POTS).Un módem analógico convierte los datos digitales de una computadora en sonido analógico y lo envía a través de las líneas telefónicas a otro módem, el cual convierte nuevamente los datos el formato digital.

❖ **Ancho de banda**

EL ancho de banda se define como la diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. El término se utiliza también para describir la medida de capacidad de caudal de un medio o protocolo de red dados.

El ancho de banda (bandwidth) es la capacidad máxima de transmisión de un enlace. Usualmente se mide en bits por segundo (bps). Es uno de los recursos más caros de toda red, el ancho de banda es una limitante para el desarrollo de aplicaciones que requieren transferir grandes cantidades de información a muchos puntos diferentes (multimedia, por ejemplo).

❖ **Anillo**

Un anillo es la conexión de una o más estaciones en una topología lógica circular. La información se transmite secuencialmente entre las estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

❖ **Anillo principal**

El anillo principal es uno de los dos anillos que conforman un anillo FDDI o CDDI. El anillo principal es la ruta por defecto para las transmisiones de datos.

❖ **Anillo secundario**

El anillo secundario es uno de los dos anillos que forman un anillo FDDI o CDDI. El anillo secundario generalmente se reserva para ser utilizado en caso de una falla del anillo principal.

❖ **ANSI**

Instituto Americano de Normas (American National Standards Institute) es una organización que desarrolla y aprueba normas de los Estados Unidos.

❖ **Aplication layer**

Capa de aplicación. En el Modelo de Referencia OSI de la arquitectura para redes de computadoras, la primera (de arriba hacia abajo) de siete capas, en donde la información se presenta al usuario.

❖ **Application Program Interface**

Interfaz para programas de aplicación API es el conjunto de convenciones de programación que definen cómo se invoca un servicio desde un programa

❖ **APPN**

Red avanzada par a par (Advanced Peer to Peer Networking).

❖ **Architecture**

Arquitectura es el diseño conceptual general de un dispositivo de hardware o red de computadoras, que especifica cómo interactuarán sus múltiples componentes.

❖ **ARCNET**

Red de computadoras con recursos asignados (Attached Resource Computer Network;). Red local desarrollada por Datapoint Corporation que utiliza una tecnología de acceso Token Passing y que tiene una velocidad de transferencia de 2.5 Mbps.

❖ **ARM**

Modo de Respuesta Asíncrono (Asynchronous Response Mode).

❖ **ARP**

Protocolo de resolución de direcciones (Address Resolution Protocol). Protocolo de Internet que se utiliza para mapear una dirección IP a una dirección
MAC.

❖ **ARP Inverso**

Protocolo de resolución de direcciones inverso RARP (Reverse Address Resolution Protocol) es un método de construcción de rutas dinámicas dentro de una red. Es un protocolo en el stack TCP/IP que brinda un método para encontrar direcciones IP en base a las direcciones MAC. Permite que un servidor de acceso descubra la dirección de red de un dispositivo asociado con un circuito virtual.

❖ **ARP Proxy**

Protocolo de resolución de direcciones Proxy es una variante del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un ruteador) envía una respuesta ARP en nombre de un nodo extremo al Host solicitante. ARP Proxy puede disminuir el uso del ancho de banda en enlaces WAN de baja velocidad.

❖ **ARPA**

Agencia de proyectos de investigación avanzada. Organización de investigación y desarrollo que es parte de DoD. ARPA es responsable de numerosos avances tecnológicos en comunicaciones y networking. ARPA se convirtió en DARPA y
luego volvió a ser ARPA nuevamente (en 1994).

❖ **ARPANET**

Red de la agencia de proyectos de investigación avanzada. Es una red de conmutación de paquetes. ARPANET fue desarrollada en los años '70 por BBN y financiada por ARPA (luego, DARPA). Finalmente, se convirtió en Internet. El término ARPANET fue retirado oficialmente en 1990.

❖ **Arquitectura abierta**

Arquitectura con la cual los desarrolladores de terceras partes pueden legalmente desarrollar productos para los cuales existen especificaciones de dominio público.

❖ **Arquitectura cliente -servidor**

Término utilizado para describir los sistemas de red de informática distribuida en los cuales las responsabilidades de la transacción se dividen en dos partes: cliente (frontal) y servidor (nodo). Ambos términos (cliente y servidor) pueden aplicarse a programas de software o a dispositivos reales de computación. Esta arquitectura también se conoce como informática distribuida.

❖ **ASCII**

Código estándar estadounidense para el intercambio de información (American Standard Code for Information Interchange). Estándar que define cómo representar dígitos, letras, signos y signos de puntuación en computadoras (por ejemplo, la A mayúscula corresponde al código número 65).

❖ **ASK**

Codificación por desplazamiento de amplitud (Amplitude-Shift Keying).

❖ **ASN**

Número de sistema autónomo (Autonomous System Number). En un sistema autónomo, una dirección IP que se ha asignado mediante un protocolo automático para una de las estaciones de trabajo de la red.

❖ **Assigned number**

Número asignado. En internet es un valor asociado con un protocolo específico controlado por la Autoridad de Números Asignados en Internet (IANA).

❖ **Asymmetrical Digital Subscriber Line**

Línea de Subscripción (abonado) Asimétrica Digital (ADSL). Es una tecnología de transmisión que permite a los hilos telefónicos de cobre convencionales transportar hasta 16 Mbps (megabits por segundo) mediante técnicas de compresión.

❖ **Asynchronous Transfer Mode**

Modo de Transferencia Asíncrona ATM. Estándar que define la conmutación de paquetes (cells -- celdas o células) de tamaño fijo con alta carga, alta velocidad (entre 1.544 Mbps. y 1.2 Gbps) y asignación dinámica de ancho de banda. ATM es conocido también como "paquete rápido" (fast packet). No confundir con Automatic Teller Machine (cajero automático).

❖ **Asynchronous**

Asíncrono o asincrónico Lo que se mantiene fuera de tiempo(de sincronía) de los pulsos de un reloj de sistema u otro dispositivo cronológico.

❖ **Asynchronus communication**

Comunicación asíncrona es un método de comunicación de datos donde la transmisión de bits no está sincronizada con una señal de reloj, sino que se lleva a efecto mediante el envío de un bit tras otro, con un bit de inicio y uno de parada para marcar, respectivamente, el principio y el final de la unidad de información.

❖ **Attenuation**

Atenuación es la pérdida de la intensidad de señal cuando los cables del sistema exceden la longitud máxima establecida en las especificaciones de la red

❖ **AUI**

Conexión de unidad de interfase (Attachment Unit Interface).

❖ **Authentication**

Autenticación o autentificación. Proceso mediante el cual se comprueba la identidad de un usuario en la red. Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

❖ **Autentícate**

Autenticar o autentificar Establecer la identidad de una persona que accede a la red de computadoras.

❖ **Autonomous system**

Sistema autónomo (AS). En topología de redes de Internet, un conjunto de ruteadores bajo el control de una sola autoridad administrativa. Dentro de un sistema autónomo, un administrador puede crear u denominar nuevos subdominios y asignar direcciones IP y nombres de dominio a estaciones de trabajo en la red.

B

❖ **Backbone**

La parte de una red que actúa como ruta primaria para el tráfico que sale y llega de otras redes con mayor frecuencia.

❖ **Banda ancha**

Un sistema de banda ancha es un sistema de transmisión que multiplexa varias señales independientes en un cable. En terminología de telecomunicaciones banda ancha es cualquier canal que tenga un ancho de banda mayor que un canal con grado de voz (4 kHz). En terminología LAN banda ancha es un cable coaxial sobre el cual se utiliza señalización analógica. También llamada banda amplia.

❖ **Banda base**

Banda base es la característica de una tecnología de red donde se utiliza sólo una frecuencia portadora. Ethernet es un ejemplo de red de banda base. También llamada banda estrecha.

❖ **Baudio**

El baudio es una unidad de velocidad de señalización que es igual al número de elementos de señal discontinua que se transmiten por segundo. Baudio es sinónimo de bits por segundo (bps), si cada elemento de señal representa exactamente 1 bit.

❖ **Binario**

Sistema de numeración que se caracteriza por unos y ceros (1 = encendido, 0 = apagado).

❖ **Bit**

Dígito binario(Binary Digit) utilizado en el sistema de numeración binaria. Puede ser 0 ó 1.

❖ **BPS**

Bits por segundo (bits per second).

❖ **Bridge**

El puente (bridge) es un dispositivo que conecta y transmite paquetes entre dos segmentos de red que utilicen el mismo protocolo de comunicaciones. El bridge opera en la capa de enlace de datos (capa 2) del modelo de referencia OSI. En general, el bridge filtra, envía o inunda una trama entrante basándose en la dirección MAC de dicha trama.

❖ **Broadcast**

La difusión o emisión se realiza con paquetes de datos que se enviarán a todos los nodos de una red. Los broadcasts se identifican por medio de direcciones de broadcast.

❖ **Byte**

Término empleado para referirse a una serie de dígitos binarios consecutivos sobre los cuales se opera como una unidad (un byte es igual a 8 bits).

C

❖ **Cable coaxial**

Es un cable que consta de un conductor cilíndrico exterior hueco que envuelve a un alambre conductor interno. En las LANs se utilizan normalmente dos tipos de cable coaxial, cable de 50 ohms que se utiliza para la señalización digital y cable de 75 ohms que se utiliza para la señal analógica y la señalización digital de alta velocidad.

❖ **Cable de fibra óptica**

El cable de fibra óptica es un medio físico capaz de conducir una transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más costoso, pero no es susceptible a la interferencia electromagnética y es capaz de transmitir mayores velocidades de datos.

❖ **Cable categoría 1.**

El cable categoría 1 es una de las cinco categorías de cableado UTP descritas en la norma EIA/TIA -568B. El cableado de categoría 1 se utiliza para comunicaciones telefónicas y no resulta adecuado para la transmisión de datos.

❖ **Cable categoría 2**

Es otra de las cinco categorías de cableado UTP descritas en la norma EIA/TIA -568B. El cableado de categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps.

❖ **Cable categoría 3**

El cable categoría 3 es otra de las cinco categorías de cableado UTP descritas en la norma EIA/TIA -568B. El cableado de categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps.

❖ **Cable categoría 4**

La cuarta categoría de cableado de las cinco categorías de cableado UTP descritas en la norma EIA/TIA -568B. El cableado de categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps.

❖ **Cableado de categoría 5**

Otra de las cinco categorías de cableado UTP descritas en la norma EIA/TIA-568B. El cableado de categoría 5 se utiliza para correr CDDI y puede transmitir datos a velocidades de hasta 100 Mbps.

❖ **Cableado del backbone.**

El cableado principal o de backbone es el cableado que permite realizar interconexiones entre los armarios para el cableado, y el POP y entre los edificios que forman parte de la LAN.

❖ **Capa de aplicación.**

La capa de aplicación es la capa 7 del modelo de referencia OSI. Esta capa proporciona servicios a los procesos de las aplicaciones (como correo electrónico, transferencia de archivos y emulación de terminal) que no pertenecen al modelo OSI. La capa de aplicación identifica y establece la disponibilidad de las partes que se tiene pensado comunicar (y de los recursos necesarios para conectarse con ellos), sincroniza aplicaciones cooperativas y aprueba los procedimientos para recuperación de errores y control de la integridad de los datos.

❖ **Capa de enlace de datos**

La capa de enlace de datos o capa 2 del modelo de referencia OSI brinda un tránsito confiable de datos a través de un enlace físico. La capa de enlace de datos tiene correspondencia con el direccionamiento físico, topología de red,, notificación de error, entrega solicitada de tramas y control de flujo. El IEEE ha dividido esta capa en dos subcapas: la subcapa MAC y la subcapa LLC.

❖ **Capa de presentación**

La capa de presentación es la capa numero 6 del modelo de referencia OSI. Esta capa garantiza que la información enviada por la capa de aplicación de un sistema sea entendible por la capa de aplicación de otro.

❖ **Capa de red**

La capa de red es la capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas terminales. La capa de red es la capa donde tiene lugar un enrutamiento. Corresponde aproximadamente a la capa de control de ruta del modelo SNA.

❖ **Capa de sesión**

Es la capa 5 del modelo de referencia OSI. Esta capa establece, gestiona y termina sesiones entre aplicaciones y gestiona el intercambio de datos entre entidades de la capa de presentación. Corresponde a la capa de control de flujo de datos del modelo SNA.

❖ **Capa de transporte**

La capa de transporte o capa 4 del modelo de referencia OSI es responsable de una comunicación de red confiable entre nodos extremos. La capa de transporte provee mecanismos para el establecimiento, mantenimiento y terminación de circuitos virtuales, detección y recuperación de fallas en el transporte y control de flujo de información.

❖ **Capa física**

Es la capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para la activación, mantenimiento y desactivación de la capa física entre sistemas finales.

❖ **CD**

Detección de portadora (Carrier Detect). Señal que indica si una interfaz se encuentra activa. También es una señal generada por un módem que indica que se ha conectado una llamada.

❖ **Circuito virtual**

Es un circuito lógico creado para garantizar una comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por medio de un par VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) y puede ser permanente (PVC) o conmutado (SVC).

❖ **Codificación**

La codificación es el proceso por el cual los bits son representados por tensiones. Son las técnicas eléctricas utilizadas para transportar señales binarias.

❖ **Código de corrección de errores**

Los códigos de corrección de errores son aquellos códigos que tienen suficiente información de señalización como para permitir la detección y corrección de muchos errores en el receptor.

❖ **Código de detección de errores**

Son los códigos que pueden detectar errores de transmisión mediante un análisis de los datos recibidos, basándose en la adherencia de los datos a pautas estructurales apropiadas.

❖ **Colisión**

La colisión en una red Ethernet, es el resultado de dos nodos transmitiendo en forma simultánea. Las tramas provenientes de cada dispositivo impactan y se dañan al encontrarse en el mismo medio físico.

❖ **Conector BNC**

Es el conector estándar (Bayote-Neill-Concelman) que se utiliza para conectar el cable coaxial 10Base2 IEEE 802.3.

❖ **Conector RJ**

Es el conector tipo ficha registrado (Register Jack). Estos conectores estándar normalmente son empleados para conectar las líneas telefónicas. Los conectores RJ se utilizan actualmente para las conexiones telefónicas y 10BaseT y para otros tipos de conexiones de red. RJ-11, RJ-12 y RJ-45 son algunos de los tipos de conectores RJ más difundidos.

❖ **Conmutador de paquetes**

Un conmutador de paquetes (packet switch) es un dispositivo WAN que enruta los paquetes a lo largo de la ruta más eficiente y permite que un canal de comunicaciones sea compartido por múltiples conexiones. Algunas veces denominado como nodo de conmutación de paquetes (PSN) y anteriormente denominado un IMP.

❖ **CRC**

La verificación por redundancia cíclica (Ciclic Redundancy Check) es la técnica de comprobación de errores en la que el receptor de la trama calcula un resto dividiendo el contenido de una trama por un divisor binario primo y compara el resto calculado con un valor almacenado en la trama por el nodo emisor.

❖ **CSMA/CD**

Método de acceso múltiple con detección de portadora y detección de colisiones (Carrier Sense Múltiple Access/Collision Detection). Mecanismo de acceso al medio en el cual los dispositivos listos para transmitir datos primero verifican el canal en busca de una portadora. Si no se detecta ninguna portadora por un lapso especificado, un dispositivo puede transmitir. Si dos dispositivos transmiten a la vez, tiene lugar una colisión y ésta es detectada por todos los dispositivos que entran en colisión. En consecuencia, la colisión demora las retransmisiones desde dichos dispositivos por un lapso al azar. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

D

❖ **Datagrama**

Un datagrama es un agrupamiento lógico de información enviada como una unidad de capa de red por un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información en la Internet. Los términos Frame, mensaje, paquete y segmento también se utilizan para describir los agrupamientos lógicos de información en las diferentes capas del modelo de referencia OSI

❖ **Demodulación**

La demodulación es el proceso de retornar una señal modulada a su forma original. Los módems realizan la demodulación, tomando una señal analógica y retornándola a su forma original (digital).

❖ **Dirección de broadcast**

La dirección de broadcast es una dirección especial reservada para enviar un mensaje a todas las estaciones. En general, la dirección de broadcast es una dirección de destino MAC con todos los bits con valor 1.

❖ **Dirección de punto**

La dirección de punto es la notación común para las direcciones IP en la forma w.x.y.z, donde cada número representa en formato decimal, 1 byte de la dirección IP de 4 bytes. También es conocida como notación de punto o notación punteada en cuatro partes.

❖ **Dirección de red**

Es la dirección de nivel de red que se refiere a un dispositivo de red lógico, en vez de físico. También llamada dirección de protocolo.

❖ **Dirección de subred**

Es la parte de una dirección IP que la máscara de subred especifica como subred.

❖ **Dominio**

Este concepto se usa en tres aspectos: 1.En Internet, es una parte del árbol de jerarquía de nombres que se refiere a los agrupamientos generales de redes basadas en tipo de organización o geografía. 2.En SNA, un SSCP y los recursos que controla. 3.En IS-IS, un conjunto lógico de redes.

❖ **Dominio de broadcast**

El dominio de broadcast es el conjunto de todos los dispositivos que recibirán tramas de broadcast provenientes de cualquier dispositivo del conjunto. Los dominios de broadcast son limitados típicamente por los ruteadores ya que éstos no envían tramas de broadcast.

❖ **Dominio de colisión**

El dominio de colisión es un área de una red Ethernet dentro de la cual se propagan los tramas que se han colisionado.

❖ **Dominio de enrutamiento**

El dominio de enrutamiento se forma por un grupo de sistemas finales y de sistemas intermedios que operan bajo el mismo conjunto de normas administrativas. Dentro de cada dominio de enrutamiento hay una o más áreas, cada una de las cuales está identificada en forma única por medio de una dirección de área.

❖ **DS-0**

El DS-0 (Digital Signal) es el nivel 0 de la señal digital. Es la especificación de entramado que se utiliza para transmitir señales digitales en un único canal a 64-kbps en una facilidad T1.

❖ **DS-1**

Un DS-1 es el nivel 1 de la señal digital. Es una especificación de entramado que se utiliza para transmitir señales digitales a 1,544-Mbps en una facilidad T1 (en los Estados Unidos) o a 2,108-Mbps o en una facilidad E1 (en Europa).

❖ **DS-3**

Un DS-3 es el nivel 3 de la señal digital. Es la especificación de entramado que se utiliza para transmitir señales digitales a 44,736-Mbps en una facilidad T3.

E

❖ **E1**

Es el sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 2,048 Mbps. Las líneas E1 se pueden arrendar de portadoras comunes para uso privado.

❖ **E3**

Es el sistema de transmisión digital de área amplia, utilizado predominantemente en Europa, que transporta datos a una velocidad de 34,368 Mbps. Las líneas E3 se pueden arrendar de portadoras comunes para uso privado.

❖ **Error de alineación**

El error de alineación se produce en redes IEEE 802.3, es un error que tiene lugar cuando la cantidad total de bits de una trama recibida no es divisible por ocho. Los errores de alineación son provocados en general por una trama dañada debido a colisiones.

❖ **Ethernet**

El estándar Ethernet es la especificación de LAN de banda base, creada por Xerox Corporation y desarrollada conjuntamente entre Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y corren por una variedad de tipos de cable a 10 Mbps. Ethernet es similar a la serie de normas IEEE 802.3.

F

❖ **Fast Ethernet**

Fast Ethernet hace referencia a cualquiera de las especificaciones de Ethernet de 100 - Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, preserva características tales como formato de trama, mecanismos MAC y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes de Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

❖ **FDDI**

Interfaz de datos distribuida por fibra (Fiber Distributed Data Interface). Norma LAN, definida por ANSI X3T9.5, que especifica una red de token-passing de 100-Mbps que utiliza un cable de fibra óptica, con distancias de transmisión de hasta 2 Km FDDI utiliza una arquitectura de anillo doble para proporcionar redundancia.

❖ **DDI II**

Es la norma ANSI que mejora FDDI. FDDI II proporciona una transmisión isócrona para circuitos de datos sin conexión y para circuitos de voz y vídeo orientados a conexión.

❖ **FDM**

La multiplexación de división de frecuencia (Frequency Division Multiplexing) es la técnica por la cual se puede asignar un ancho de banda a información desde varios canales en un único cable, basándose en la frecuencia.

❖ **Fragmentación**

Proceso de dividir un paquete en unidades más pequeñas cuando se transmite por un medio de red que no puede soportar el tamaño original del paquete.

❖ **Frame**

Una trama o frame es una agrupación lógica de información, enviada como unidad de la capa de enlace de datos por un medio de transmisión. A menudo, se refiere al encabezado y al trailer, utilizados para la sincronización y el control de errores, que rodean a los datos del usuario que contiene la unidad. Los términos Datagrama, mensaje, paquete de datos y segmento también se utilizan para describir agrupaciones lógicas de información en diversas capas del modelo de referencia OSI.

❖ **Frame Relay**

El protocolo de conmutación de tramas (Frame Relay) es el protocolo de la capa de enlace de datos conmutados, de norma industrial, que administra varios circuitos virtuales utilizando una encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficaz que X.25, el protocolo para el cual se considera por lo general un reemplazo.

G

- **Gateway**

El termino gateway en el ambiente IP, es un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, se utiliza el término ruteador para describir los nodos que realizan esta función, mientras que gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

H

- **Half dúplex**

La transmisión half duplex tiene capacidad de transmisión de datos solamente en una dirección a la vez, entre una estación de envío y una estación de recepción.

- **H.323**

Protocolo que proporciona calidad en el servicio QoS (Quality of Service).

- **Host**

Un host o anfitrión es un término usado en los sistemas de computación en una red. Es similar al término nodo excepto que el host usualmente implica un sistema de computación, mientras que un nodo generalmente se aplica a cualquier sistema en red, incluyendo los servidores de acceso y ruteadores.

- **Hub**

El dispositivo concentrador (Hub) puede tener tres significados: 1.) En forma general, es un término utilizado para describir un dispositivo que sirve como centro de una red de topología en estrella. 2.)Es un dispositivo de hardware o software que contiene múltiples módulos independientes pero conectados de equipo de red e internetworking. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten, sino que meramente dividen las señales enviadas a través de ellos). 3.) En Ethernet e IEEE 802.3, un repetidor Ethernet multipuerto, algunas veces denominado como concentrador.

- **Hub activo**

Un hub activo es un dispositivo de varios puertos que amplifica las señales de transmisión LAN.

I

- **Internet.**

Internet es un termino utilizado para referirse a la mayor red de internetworking (interconexión) global que conecta a decenas de miles de redes de todo el mundo y que tiene una "cultura" que apunta básicamente a la investigación y a la estandarización basándose en el uso en la vida real. Muchas tecnologías de red líderes provienen de la comunidad de Internet. La Internet surgió a partir de la ARPANET. Antes llamada también Internet DARPA. No debe confundirse con el término general Internet.

- **InterNIC**

El centro de información de redes de Internet (Internet Network Information Center) es una organización que sirve a la comunidad de Internet brindando asistencia al usuario, documentación, capacitación, servicio de registro de nombres de dominio de Internet y otros servicios. Antiguamente llamado Network Information Center (NIC) (Centro de Información de Redes).

❖ **IP**

El Protocolo Internet es el protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetworking (interconexión) sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y reensamblado y seguridad. Documentado en RFC 791.

L

❖ **LAN**

Las redes de área local (Local Area Network) son red de datos de alta velocidad y bajos niveles de error que cubren un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas física y de enlace datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

❖ **LLC**

La subcapa de control de enlace lógico (Logical Link Control) es la más alta de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa LLC maneja el control de errores, el control de flujo, el entramado y el direccionamiento de subcapa MAC. El protocolo LLC que más prevalece es IEEE 802.2, que incluye tanto la variante sin conexión como la orientada a conexión.

M

❖ **MAC**

La subcapa de control de acceso al medio es la inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos, por ejemplo, define si se utilizará token passing o contención.

❖ **MAN**

La red de área metropolitana (Metropolitan Area Network) es una red que abarca un área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN.

❖ **Máscara de dirección.**

La mascara de dirección es un conjunto de bits que se utiliza para describir qué porción de una dirección se refiere a la red o subred y cuál parte se refiere al Host. A veces se le llama simplemente máscara.

❖ **Máscara de subred**

La mascara de subred es una máscara de dirección de 32 bits que se utiliza en el IP para indicar los bits de una dirección IP que se están utilizando para la dirección de subred.

❖ **Modelo de referencia OSI**

Modelo de referencia de interconexión de sistemas abiertos (Open System Interconection) es un modelo de arquitectura de redes desarrollado por ISO e ITU-T. El modelo consiste en siete capas, cada una de las cuales especifican funciones particulares de la red, como por ejemplo direccionamiento, control de flujo, control de errores, encapsulación y transferencia confiable de mensajes. La capa superior (capa de aplicación) es la más próxima al usuario; la capa inferior (capa física) es la más próxima a la tecnología de medios. La capa siguiente a la capa inferior está implementada en hardware y en software mientras que las cinco capas superiores están implementadas únicamente en software.

❖ **Módem**

Un Modulador-demodulador es un dispositivo que convierte señales digitales y análogas. En el punto de origen, un módem convierte señales digitales a una forma apropiada para la transmisión por facilidades de comunicación análogas.

❖ **Multicast**

Los paquetes multicast son paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

❖ **MPLS**

La conmutación de etiquetas multiprotocolo (Multi Protocol Label Switching) es la integración de protocolos.

N

❖ **N7**

Señalización por canal común.

❖ **NetBIOS**

El sistema de básico de entrada/salida de red (Network Basic Input Output System) es una API utilizada por aplicaciones en una LAN IBM para solicitar servicios de procesos de red de menor nivel. Estos servicios podrían incluir inicio y terminación de sesiones y transferencia de información.

❖ **Networking**.

El termino networking hace referencia a la conexión de cualquier conjunto de computadoras, impresoras, ruteadores, switches y otros dispositivos, con el fin de enviar información por un medio de transmisión.

❖ **NIC**

La tarjeta de interfaz de red (Network Interface Card) es una tarjeta que provee capacidades de comunicación de red hacia y desde un sistema de
computación. También llamada adaptador.

❖ **Nodo**

Un nodo es el punto final de una conexión de red, o unión común a dos o más líneas en una red. Los nodos pueden ser procesadores, controladores, o estaciones de trabajo. Los nodos, que pueden variar según su capacidad de enrutamiento y otras capacidades funcionales, pueden estar interconectados por enlaces y servir como puntos de control en la red. El término nodo se emplea a veces de modo genérico para indicar cualquier entidad que puede tener acceso a una red y es utilizado a menudo en forma intercambiable con dispositivo.

❖ **Número de Host**

Es la parte de una dirección IP que designa qué nodo se está direccionando en la subred.. a veces también se le conoce como dirección de host.

P

❖ **Paquete**

Un paquete es un agrupamiento lógico de información que incluye un encabezado que contiene información de control y (usualmente) datos del usuario. Los paquetes se utilizan más frecuentemente para hacer referencia a las unidades de datos de las capas de red.

❖ **Par trenzado.**

El cable de par trenzado es un medio de transmisión de velocidad relativamente baja que consiste en dos cables aislados, dispuestos en forma de espiral regular. Los cables pueden

ser blindados o sin blindaje. Par trenzado es común en aplicaciones telefónicas y es cada vez más común en redes de datos.

❖ **Portadora**

La portadora es una onda electromagnética o corriente alterna de frecuencia única, apropiada para la modulación por otra señal, que transporte datos.

R

❖ **RFC**

Las peticiones de comentarios (Request for Comments) son una serie de documentos empleada como medio de comunicación primaria para transmitir información acerca de la Internet. Algunas RFC son designados por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son históricas. Las RFCs pueden encontrarse en línea en distintas fuentes.

❖ **Ruteador**

Un router es un dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los ruteadores envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado gateway (aunque esta definición de gateway va cayendo en desuso día a día).

S

❖ **Señal digital**

Señales usadas principalmente entre computadoras que constan solamente de dos estados, encendido y apagado, los cuales se indican mediante una serie de impulsos de tensión.

❖ **Señalización**

La señalización es un proceso que consiste en enviar una señal de transmisión sobre un medio físico a los fines de la comunicación.

❖ **Servidor de acceso**

Un servidor de acceso es un procesador de comunicaciones que conecta dispositivos asíncronos con una LAN o WAN mediante una red y un software de emulación de terminal. Realiza tanto enrutamiento asíncrono como síncrono de los protocolos soportados. También se le conoce como servidor de acceso a la red.

❖ **Servidor de Comunicaciones**

Un servidor de comunicaciones es un procesador de comunicaciones que conecta dispositivos asíncronos a una LAN o WAN a través de un software de red y emulación de terminal. Lleva a cabo solamente un enrutamiento asíncrono de IP e IPX.

❖ **Servidor de impresión**

Es un sistema de computación en red que registra, administra y ejecuta (o envía para ejecución) solicitudes de impresión desde otros dispositivos de red.

❖ **SIP**

Protocolo de iniciación de sesión (Session Initiator Protocol).

❖ **SMTP**

El protocolo de transferencia de correo (Simple Mail Transfer Protocol) es un protocolo de Internet que brinda servicios de correo electrónico.

❖ **SNMP**

Protocolo simple de administración de redes (Simple Network Management Protocol) es protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El

SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y
seguridad.

- **SNMP2**

La versión 2 del protocolo de administración de red SNMP2 soporta estrategias de gestión de redes tanto centralizadas como distribuidas, e incluye mejoras al protocolo SMI, a las operaciones del protocolo, a la arquitectura de gestión y a la seguridad.

- **SONET**

La Red óptica síncrona (Synchronous Optical Network) es una especificación de red síncrona de alta velocidad (hasta 2,5 Gbps) desarrollada por Bellcore y diseñada para correr por una fibra óptica. STS-1 es el bloque de construcción básico de SONET. Aprobado como estándar internacional en 1988.

- **Subred**

El termino subred puede tener los siguientes significados: 1. En redes IP, es una red que comparte una dirección de subred particular. Las subredes son redes segmentadas arbitrariamente por un administrador de red para brindar una estructura de enrutamiento multinivel, jerárquico, protegiendo a la subred de la complejidad del direccionamiento de las redes conectadas. Llamada a veces subnet. 2. En las redes OSI, grupo de ES e IS bajo el control de un único dominio administrativo que utilizan un mismo protocolo de acceso a la red.

T

- **TCP/IP**

Conjunto de protocolos de Internet.

- **T1 canalizado**

Es un enlace de acceso que opera a 1,544 Mbps, que se encuentra subdividido en 24 canales (23 canales B y un canal D) de 64 Kbps cada uno. Los canales o grupos de canales individuales se conectan a diferentes destinos. Soporta DDR, Frame Relay
y X.25. También denominado T1 fraccionario.

- **T3**

Es una facilidad de portadora de WAN digital. T3 transmite datos formateados en DS-3 a 44.736 Mbps por la red de conmutación telefónica.

U

- **UDP**

El protocolo de datagrama de usuario (User Datagram Protocol) es un protocolo sin conexión de capa de transporte en el stack de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

W

- **WAN**

La red de área amplia (Wide Area Network) es una red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

❖ **WAP**

Protocolo Móvil (Wireless Access Protocol).

Numero

❖ **10Base2**

La especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial delgado de 50 ohms. 10Base2, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 185 metros por segmento.

❖ **10Base5**

Es la especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial estándar (grueso) de 50 ohms. 10Base5, que forma parte de la especificación de capa física de banda base IEEE 802.3, tiene un límite de distancia de 500 metros por segmento.

❖ **10BaseF**

Otra especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BaseFB, 10BaseFL y 10BaseFP para Ethernet a través de cableado de fibra óptica.

❖ **10BaseFB**

Una especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFB forma parte de la especificación IEEE 10BaseF. No se utiliza para conectar estaciones de usuario, sino para brindar un backbone de señalización síncrona que permita que los segmentos y repetidores adicionales estén conectados a la red. Los segmentos 10BaseFB pueden tener una longitud de hasta 2.000 metros.

❖ **10BaseFL**

Es una especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFL forma parte de la especificación IEEE 10BaseF y, al poder interoperar con FOIRL, está diseñada para reemplazar a la especificación FOIRL. Los segmentos 10BaseF pueden tener una longitud de hasta 1.000 metros si se los utiliza con FOIRL y de hasta 2.000 metros si se utiliza exclusivamente 10BaseFL.

❖ **10BaseT**

Especificación Ethernet de banda base de 10 Mbps que utiliza dos pares del cableado de par trenzado (Categoría 3, 4 ó 5) un par para transmitir datos y el otro para recibir datos. 10BaseT, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia aproximado de 100 metros por segmento.

❖ **10Broad36**

Es una especificación Ethernet de banda ancha de 10 Mbps que utiliza cable coaxial de banda ancha. 10Bro ad36, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 3.600 metros por segmento.

❖ **10 Mbps**

10 millones de bits por segundo. Unidad de velocidad de transferencia de información. Ethernet porta 10 Mbps.

❖ **100BaseFX**

Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una correcta temporización de la señal, un enlace 100BaseFX no puede exceder los 400 metros de longitud. Basada en el estándar IEEE 802.3.

❖ **100BaseT**

Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la cual se base 100BaseT envía impulsos de enlace a

través del segmento de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen más información que los utilizados en 10BaseT. Esta especificación se basa en el estándar IEEE 802.3.

- **100BaseT4**

Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cuatro pares del cableado UTP Categoría 3, 4 ó 5. Para garantizar una correcta temporización de las señales, un segmento 100BaseT4 no puede exceder los 100 metros de longitud. Basada en el estándar IEEE 802.3.

- **100BaseTX**

Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares del cableado UTP o STP. El primer par de cables se emplea para recibir datos y el segundo para transmitir. Para garantizar una correcta temporización de las señales, un segmento 100 Base TX no puede exceder los 100 metros de longitud. Basada en la norma IEEE 802.3.

- **100BaseX**

Especificación Fast Ethernet de banda base de 100 Mbps que se refiere a los estándares 100BaseFX y 100BaseTX para Fast Ethernet sobre cableado de fibra óptica. Basada en el estándar IEEE 802.3.

- **100VG-AnyLAN**

Tecnología de medios Fast Ethernet y Token Ring de 100 Mbps que utiliza cuatro pares del cableado UTP Categoría 3, 4 ó 5. Esta tecnología de transporte de alta velocidad, desarrollada por Hewlett -Packard, puede hacerse funcionar sobre redes Ethernet 10BaseT existentes. Basada en el estándar IEEE 802.12.

Bibliografía y referencias electrónicas

Libros

- B. P. Lathi, Sistemas de Comunicación. Ed. McGraw Hill.
- Corner, Douglas E. Redes Globales de Información con Internet y TCP/IP. Ed. Prentice may Hispanoamericana.
- Comer, Douglas E. "Internetworking with TCP/IP Volume I, Principles, protocols, and Architecture". Editorial Prentice Hall.
- Ford Merilee, Kim Lew Tecnología de Interconectividad de Redes. Ed. Prentice Hall Hispanoamericana.
- Fried E. George, Fike John L., Bellamy John C. A fondo: Transmisión de Datos y Comunicaciones. Ed. Anaya.
- Friend George. Transmisión de Datos y Comunicaciones. Ed. Anaya Multimedia.
- García Jesús, Raya José Luis, Raya Víctor Alta Velocidad y Calidad de Servicio en Redes IP. Ed. Alfaomega.
- García Jesús, Ferrando Santiago y Piattini Mario Redes para Proceso Distribuido. 2ª Edición. Ed. Alfaomega.
- Martín James. Systems Análisis for Data Transmissión. Ed. Prentice Hall.
- Parnell Teré. Guía de Redes de Alta Velocidad. McGraw-Hill.
- Raya José Luis. Redes Locales y TCP/IP. Ed. Alfaomega Grupo Editor S.A. de C.V.
- Schwartz Misha Transmisión de Información, Modulación y Ruido. Ed. McGraw Hill.
- Strembler Ferrel Sistemas de Comunicación. Fondo Educativo Interamericano.
- Silvano Gai, Internetworking IPv6 with Cisco Routers. Politecnico Di Torino.
- Cisco IOS Learning Services. The ABCs of IP Version 6.
- Tanenbaum Andrew, Redes de Computadoras, Ed. Prentice Hall.
- Keith O'Brien, Configuring Cisco Voice over IP, Global Knowledge Professinal Referente.
- Stephen A. Thomas. IPng and the TCP/IP Protocols. Implementing the Next Generation Internet. John Wiley & Sons Inc.

Manuales de Cursos

- Alcatel. Diplomado en nueva generación de redes & e-Business. Modulo I. Redes de datos, Modulo II. Tecnología de redes de área local, Modulo V. TCP/IP & routing. Modulo VIII. Convergencia e Internet, Modulo IX. Arquitectura de Internet & e-business.
- Netscreen. Implementing Netscreen Security Gateways. Cap. 3 Security concepts for IP networks, Cap. 13 IPSEC Concepts.
- Novell Education. IntranetWare Course 200 Networking Technologies. Section 3 Transmission Media, Section 4 Transmission Media Connection, Section 5 Networks Protocols and Models, Section 6 The OSI Physical Layer, Section 7 The OSI Data Link Layer, Section 8 The OSI Network Layer, Section 9 The OSI

Transport Layer, Section 10 The OSI Session Layer, Section 11 The OSI Presentation Layer, Section 12 The OSI Application Layer, Section 13 Internet Protocol.
- Tecnyce. Seminario de TCP/IP.

White Papers

- Antennas for Wireless Networks.
- Consulintel. Guia didactica de Fast Ethernet.
- Chisholm Leigh Anne. CCNA LAN Switching.
- Chisholm Leigh Anne. Layer 2 Switching and Bridging.
- Dale Holmes. A Begeinner´s Look at WAN Technologies.
- Dennis Laganiere. Networking without a NET.
- Howard C. Berkowitz. Internet routing with BGP Part I, II y III.
- Howard C. Berkowitz. IPv6 Basic Services.
- Howard C. Berkowitz. OSI and Standards.
- Howard C. Berkowitz. OSPF, parts I y II.
- Howard C. Berkowitz. Topology and IP Addressing: The CCNA Perspective.
- Jasón Sinclair. CCNA IP Routing.
- Jason Sinclair. EIGRP.
- Katherine Tallis. OSI Reference Model.
- Kevin Downes. Network Address Translation.
- Leigh Anne Chisholm. Layer 2 Switching and Bridging.
- Leigh Anne Chisholm. CCNA LAN Switching.
- Lugo Luinis Alberto. Introducción a las Redes
- Marc Menninger. Physical Internetworking and Industry Standards for Networks.
- OSPF Protocol Mechanisms.
- Rita Pusmanova. RIP.
- Trinexus. Conceptos básicos de Bridging
- Trinexus. Conceptos Básicos de Routing, IP e IPX.
- Trinexus. Conceptos básicos de Ethernet e Internetworking.
- Wireless Design.

Referencias electrónicas

- www.cybercursos.net Switches y ruteadores.
- www.lpis.com Curso sobre redes I
- www.geocities.com Introducción a las redes.
- www.cybercursos.net Componentes de una red.
- www.cybercursos.net. Medios de transmisión.
- www.consulintel.es Fast Ethernet
- www.rad.com Glosario
- www.rad.com The OSI Reference Model.
- www.rad.com Modems.
- www.monografias.com Protocolos de red. Protocolos TCP/IP.
- www.rad.com. Digital Communicatios.
- www.rad.com. Digital Encoding.

- www.cybercursos.net. Manual de Protocolos.
- www4.uji.es Protocolos TCP/IP
- www.gare.co.uk Synchronous Digital Hierarchy (SDH).
- www.rad.com. OSPF
- www.rad.com. Token Ring.
- www.consulintel.es. Guía didáctica de Ethernet.
- http://ipv6.research.microsoft.com/ Sitio web con IPv6 nativo de investigación de Microsoft.
- www.freesoft.org
- www.ipv6.unam.mx/
- www.portalv6.com
- www.reuna.cl
- www.consulinterl.eruro6ix.org
- www.deepspace6.net
- www.mundotutoriales.com
- 6net.if.hu/ipv6.apps
- www.ripe.net
- www.6sos.org
- www.ipv6style.jp
- www.ist-ipv6.org
- www.join.uni-muenster.de
- ftp.kame.net
- http://ipv6.uk.ntt.net
- www.kfu.com
- www.ipv6.retina.ar
- ftp://rohan.umu.euro6ix
- tb4.consulintel.euro6ix.org
- www.ipv6.udg.mx
- http://imasd.elmundo.es
- www.cisco.com/ipv6
- Microsoft IPv6 Web site
- www.microsoft.com/windowserver2003/tecnologies/ipv6
- http://msdn.microsoft.com
- http://altavista.ipv6.digital.com/
- http://www.ipv6forum.com/
- http://www.6bone.net/
- http://www.kame.net/
- http://carmen.ipv6.cselt.it:8090/ipv6/
- http://www6.ipv6.polito.it/
- http://www.ipv6.itesm.mx/
- ftp://r6d6.ipv6.itesm.mx/
- ftp://ftp.stealth.net/
- www.lacnic.net
- http://www.research.microsoft.com/msripv6
- http://www.internic.net
- http://www.ietf.org
- http://www.iab.org