UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CIUDAD UNIVERSITARIA

GUÍA PARA EL DISEÑO DE REDES LAN

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN TELECOMUNICACIONES

PRESENTAN:

FERNANDO TOLENTINO DELGADILLO
MAXIMINO VENEGAS REYES

DIRECTOR DE TESIS
ING. ADALBERTO FRANCISCO GARCÍA ESPINOSA
DEPARTAMENTO DE TELECOMUNICACIONES

MÉXICO, D. F., MAYO 2005.

A mis Padres y Hermanos

Sabiendo que jamás existirá una forma de agradecer en esta vida de lucha y de superación constante, deseo expresarles que mis ideales, esfuerzos y logros han sido también suyos y constituye el legado más grande que pudiera recibir.
¡Con cariño, admiración y respeto!

A mis Amigos y Profesores

Durante esta etapa universitaria quiero agradecer a todas aquellas personas que formaron parte de mi entorno académico y que con su trabajo, dedicación y esfuerzo colaboraron para lograr este objetivo.
¡México, Pumas, Universidad!

Fernando Tolentino Delgadillo

Agradecimientos

Este trabajo concluye la etapa más importante en la formación profesional y personal de mi vida; y es gracias a mis padres, a mi tío, a mis hermanos, a mi novia, a mis amigos y compañeros, profesores, y por supuesto, a la Facultad de Ingeniería de la Universidad Nacional Autónoma de México por brindarme la oportunidad, apoyo, tiempo, esfuerzo, recursos, confianza, y sobre todo, su comprensión. Todo ello ha fortalecido mi criterio, mis principios y valores, ha ampliado mis conocimientos, ha cambiado mi manera de pensar (proporcionándome un panorama impresionante de posibilidades), ha provocado que sea más conciente de los problemas sociales, culturales y económicos que existen en el País y en el Mundo, y lo que más me llena de satisfacción, es que me ha hecho una persona productiva y útil para México.

México, Pumas, Universidad!!!

Maximino Venegas Reyes

Índice

Introducción

El presente trabajo tiene como objetivo primordial el proporcionar una guía para el diseño de redes LAN que tiene gran utilidad para aquellas personas que se van iniciando en el diseño de redes LAN. Contiene una amplia información teórica de las tecnologías y protocolos más comunes, que servirán como base para llevar a la práctica estos conocimientos, y así diseñar una red con características específicas, como la disponibilidad, redundancia, desempeño, flexibilidad, confiabilidad, escalabilidad, costo y administración, satisfaciendo cada uno de los requerimientos y necesidades del usuario.

Esta Tesis se encuentra dividida en 6 grandes temas capitulados y estructurados de la manera siguiente:

Un Marco Teórico que es de vital importancia como antecedente para el entendimiento de este trabajo, en el se presenta e inicia con el Modelo de Referencia OSI, el cual tiene por objetivo ser la referencia para la interconexión de sistemas abiertos, por ejemplo: protocolos y redes de datos. Las funciones de cada una de sus siete capas y su importancia en el proceso de comunicación entre distintos sistemas, así como sus características más importantes. Aprovechando ésta referencia del Modelo OSI, después se describen las normas para la implementación del Cableado Estructurado para edificios y la administración de esta infraestructura. Se describen las Tecnologías para redes LAN más comunes en el mercado y que actualmente se encuentran implementadas, en primer término se trata la tecnología Ethernet: sus fundamentos, elementos, técnica de acceso al medio, los distintos formatos de tramas Ethernet, sus implementaciones físicas y la evolución de Ethernet. Posteriormente, se aborda la tecnología VLAN definida en la norma IEEE 802.1Q, donde se muestra el proceso de microsegmentación de red LAN, formatos de etiquetado y cambios en la trama 802.3, y los diferentes tipos de conexión lógica. No se pueden dejar atrás las WLAN, aquí se mencionan las variaciones de la norma IEEE 802.11, la capa física, la subcapa MAC, la trama y la estructura de red. Otra parte fundamental, que no se debe omitir en este trabajo son los Dispositivos de Interconexión de Red: repetidores, concentradores, bridges, switches, enrutadores, de los cuales se mencionan sus principales características, funciones y la capa del modelo OSI en la cual operan, así como el algoritmo STP utilizado en esquemas de redes redundantes. La suite de protocolos TCP/IP y sus características funcionales, direccionamiento lógico y los formatos de encabezado. Para poder comunicar lógicamente las redes LAN, los Protocolos de Enrutamiento IP: ARP, Proxy ARP, Gratuitous ARP, tipos de enrutamiento, RIP y OSPF. Finalmente, algunas aplicaciones que dan valor agregado a las redes de datos, Red Multiservicios: VoIP, Videoconferencia (H.323), Streaming, etc.

Entrando en materia con el diseño, en el segundo capitulo se describen los modelos para el diseño de la topología de red, los beneficios y características. Es evidente que este capitulo da la pauta para la guía de diseño de red, ya que depende de los requerimientos de diseño del usuario, por ejemplo: la flexibilidad, el costo, disponibilidad, redundancia, etc. Por otra parte, es la base para el despliegue del Cableado Estructurado como parte importante de la infraestructura de red. Este capitulo se describen tres modelos: Modelo de Diseño Jerárquico, Modelo de Redundancia y Modelo Seguro.

Al igual que en el capitulo anterior, el tercer capitulo Modelo de Diseño del Campus, comprende la parte física del diseño de red, haciéndose énfasis en el Backbone y diversas maneras de implementarlo. Estos modelos de diseño definen la ubicación de los

closets de comunicaciones MDF e IDF, los medios físicos para el backbone: *backplane* de algún switch o enrutador, fibra óptica o cobre, así como los dispositivos de interconexión entre los diferentes puntos de interés (edificios, campus, sitios u oficinas remotas, etc.). Además, se abordan los puntos más importantes de cada diseño, así como sus ventajas y desventajas, y en que caso se debe usar uno sobre otro.

El capitulo de Guía de Diseño de Red, es la esencia de esta tesis, ya que es el que permite obtener e identificar los requerimientos para el diseño o reestructuración de la red de datos en cuestión, por ello se detallan procedimientos secuénciales que van de lo trivial a lo complejo. También, se dan formatos o *checklist* para alcanzar los objetivos de estos procedimientos derivados de las mejores practicas (*best practices*). Esta guía es de suma importancia para la planeación y diseño de la red de datos, por esta razón, se ha dividido en nueve temas. La caracterización de la red existente es el punto medular para obtener los requerimientos del usuario, porque generalmente, él mismo los desconoce, por está razón se han desarrollado 12 pasos a seguir para poder obtener esta información y tener una visión amplia a cerca del estado operacional de la red. El siguiente tema tiene por objetivo obtener las nuevas necesidades del usuario, donde se destacan las limitantes del negocio con respecto a las Tecnologías de Información y Comunicaciones. Todo diseño de topología está basado en el modelo de referencia OSI, como ya se comento anteriormente. Se han descrito varios modelos en el capítulo 2 donde se mencionan las características de cada modelo, y que de acuerdo con éstas y la caracterización de la red o las necesidades, se utilizará un modelo o incluso una combinación de ellos. Otra consideración que es importante tomar en cuenta, es el Hardware a utilizar en el diseño, realizando una comparación entre dos dispositivos de interconexión, como son los switches y enrutadores. El direccionamiento de red, es parte estructural del diseño lógico de la red y debe cumplir con los alcances desarrollados en este tema: identificar los procesos para diseñar un modelo de direccionamiento de red escalable y proponer un esquema de nombres para hosts con la finalidad de facilitar la administración y ayudar a la identificación de problemas. Para dar consistencia en la interconexión de redes, es necesario identificar y seleccionar los protocolos de enrutamiento y bridging adecuados que satisfagan los requerimientos de desempeño, seguridad y capacidad, todo esto, es descrito en el tema que lleva por nombre: Seleccionando Protocolos de Enrutamiento y Bridging. Una vez que se obtiene el diseño de la red, es indispensable disponer de una buena estrategia de administración de la red la cual permitirá una alta disponibilidad del servicio. El resultado final del diseño de la red, debe ser documentado y para ello se proporcionan los puntos más relevantes que debe de incluir dicho documento. Como último punto de este capítulo, se encuentra la Validación del Diseño de Red, y juega un papel importante respecto a los alcances y objetivos del diseño de red para que cumplan con los requerimientos del usuario, la forma de conseguirlo, es proporcionar algunas recomendaciones a cerca de la construcción de prototipos y pilotos del diseño que conducen a pruebas reales del funcionamiento y permite palpar los requerimientos.

Dependiendo del tipo de requerimientos, por ejemplo, las aplicaciones en tiempo real como la VoIP, necesitan contar con esquemas que garanticen la comunicación, este objetivo solo es posible cuando hay una diferenciación de tráfico, y la única manera de realizarlo es con la Calidad de Servicio. En el capítulo cinco se describen los mecanismos utilizados en la capa 2 y 3 del modelo de referencia OSI para cumplir con esa tarea. Además, se estudian las técnicas de encolamiento, basadas en normas, que utilizan los distintos dispositivos de interconexión.

No menos importante, también se hace referencia a un capítulo que en esencia no es parte del diseño, pero que da un panorama para detectar y solucionar posibles fallas una vez que se ha realizado un prototipo o piloto, o que incluso se ha puesto en funcionamiento el diseño de red. Esto es posible gracias a la explicación de un modelo general para la resolución de problemas, la prevención de fallas, las herramientas para la resolución de problemas, SNMP y formatos que pueden ser utilizados para registrar estos eventos. Todo ello con un enfoque de los protocolos y tecnologías descritas en el presente trabajo.

Finalmente, se describen los puntos de mayor importancia y que proporcionaron demasiado valor a este documento, así como recordatorios que resumen todo este trabajo que solo tiene la finalidad de ser una Guía para el Diseño de Redes LAN.

1. Marco Teórico

1.1 Modelo de Referencia OSI

El modelo de referencia OSI es la arquitectura de red actual más prominente. El objetivo de éste es el de desarrollar normas para la interconexión de sistemas abiertos (Open System Interconnection, OSI). El término OSI es el nombre dado a un conjunto de normas para las comunicaciones entre hosts, terminales y redes. OSI es un modelo de 7 capas (Figura 1), donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en un host, pueda comunicarse con un proceso similar en otro host, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. El modelo es considerado como un modelo de arquitectura para comunicaciones entre hosts, y es usado como referencia en la comparación de diferentes tecnologías.

Figura 1.Las siete capas del Modelo de Referencia OSI.

La comunicación que procede de una capa del modelo, generalmente se da con otras tres capas: la capa inmediata superior, la capa inmediata inferior y la capa análoga (o peer) en el dispositivo al que se comunicará.

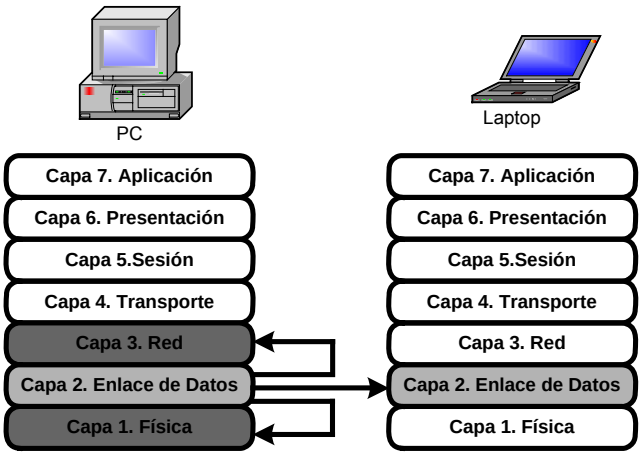


Figura 2. Comunicación entre capas en el Modelo de Referencia OSI.

La comunicación entre capas de un mismo sistema se da en términos de los servicios que ofrece una capa a su capa inmediata superior, y de los servicios que obtendrá de la capa inmediata inferior. Los puntos de conexión entre capas son llamados "SAP" (*Service Access Point*) y son usados para intercambiar información entre funciones o entidades de capas contiguas.

Las siete capas del modelo usan información de control para comunicarse con otras capas. Esta información de control toma las formas de encabezado y/o colas. El encabezado es información añadida al principio de los datos, mientras que las colas consisten en información añadida al final de los mismos al pasar de capas superiores a capas inferiores del modelo de referencia (Figura 3), este proceso se llama encapsulamiento.

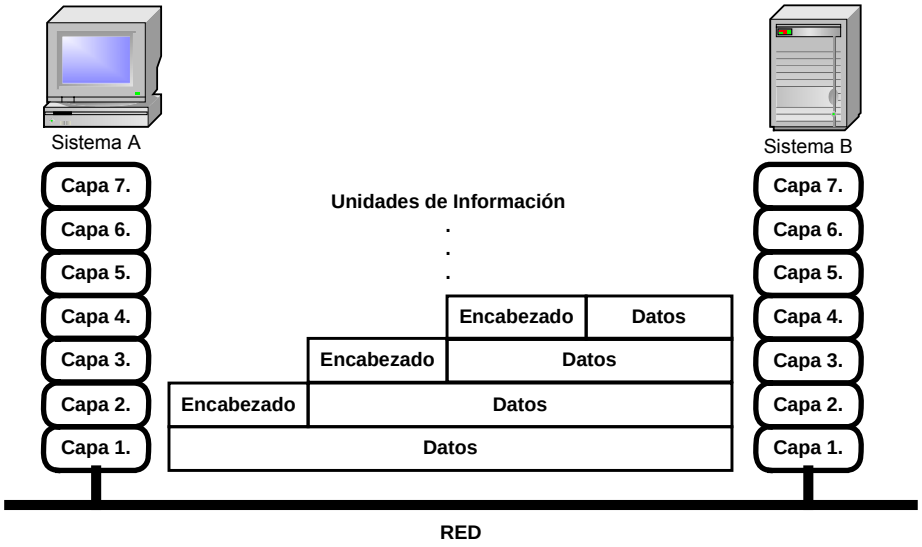


Figura 3. Adición de Información de Control entre capas.

La interpretación de la información de control es siempre entre capas del mismo nivel.

Las cuatro capas inferiores, conocidas como "capas de flujo de datos", definen la manera en que los hosts establecen conexiones unos con otros para poder intercambiar datos. Las tres capas superiores, conocidas como "capas de aplicación", definen la comunicación entre las aplicaciones de los hosts que se comunican entre sí y con los usuarios.

1.1.1 Funciones de las Capas del Modelo OSI

1.1.1.1 Capa Física

Esta capa define las especificaciones mecánicas, eléctricas y funcionales para activar, mantener y desactivar un enlace físico entre sistemas de comunicación. Relaciona la agrupación de circuitos físicos a través de los cuales los bits son movidos y que encierran

las características físicas, eléctricas funcionales y de procedimiento, para el envío y recepción de bits.

Los propósitos de la capa física son los siguientes:

- Define las características físicas (componentes y conectores mecánicos).
- Define las características eléctricas (niveles de voltaje).
- Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter. Transmisión de flujo de bits a través del medio. No existe estructura alguna.
- Maneja voltajes y pulsos eléctricos.
- Especifica cables, conectores y componentes de interfaz con el medio de transmisión. Por ejemplo RS-232, RS-449, V.35 y G.703.

1.1.1.2 Capa de Enlace de Datos

Esta capa provee un transito confiable de datos a través del enlace físico. La capa de enlace de datos detecta y corrige posibles errores que pueden ocurrir en la capa física. Además, la capa de enlace de datos permite que la capa de red controle la interconexión de los circuitos de datos con la capa física.

Este nivel se relaciona con el envío de bloque de datos sobre una comunicación física, determina el principio y el fin de un bloque de datos transmitido, detecta errores de transmisión, controla muchas máquinas que comparten un circuito físico para que sus transmisiones no sufran mezclas, direcciona un mensaje a una máquina entre varias.

Las funciones principales de la capa de enlace son las que a continuación se mencionan:

- Direccionamiento físico
- Topología de red
- Detección y control de errores (mediante el empleo del CRC).
- Control de secuencia.
- Control de flujo.
- Control de enlace lógico.
- Control de acceso al medio.
- Sincronización de la trama.
- Estructura el flujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits: encabezado y cola (trailer).
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).
- Utiliza la técnica de "piggybacking".

El piggybacking, o utilización de parte de un paquete de datos para enviar asentimientos de paquetes anteriormente recibidos, reduce, en principio, el tráfico, pero puede dar lugar a retransmisiones que contribuyan a la congestión. Transporta de acuses de recibo (acknowledgments) con el paquete de datos para ahorrar ancho de banda de la red.

Para poder proveer las funciones anteriores la IEEE tiene dos subcapas: Media Access Control (MAC), que es la norma 802.3 y Logical Link Control (LLC), norma 802.2. Además se tiene los siguientes protocolos de capa 2: Address Resolution Protocol (ARP), High Level Data Link Control (HDLC), PPP, SLIP, CSMA, CSMA/CD, SDLC, Trama Relay, ATM.

1.1.1.2.1 Códigos CRC

Uno de los métodos más usados es el código polinomial también llamado el *Cyclic Redundancy Code,* o CRC. Se trata las cadenas de bits como polinomios con coeficientes de solamente 0 y 1. Un mensaje de k bits con un *grado* de k-1 corresponde a

$$bit_0x^{k-1} +...+ bit_nx^{k-1-n} +...+ bit_{k-1}x^0$$

La aritmética con estos polinomios es módulo 2 sin llevar, es decir, la adición y la sustracción son equivalentes a XOR. La división usa XOR en ves de sustracción y A se divide en B si el número de bits en B es mayor de o igual a el número en A. El emisor y el receptor usan el mismo *polinomio de generación,* G(x), con bits alto y bajo de 1. Para calcular el checksum de r bits, que también es el grado de G(x),

1. Añade r bits de 0 a M(x), el mensaje, produciendo $x^rM(x)$.
2. Divide $x^rM(x)$ por G(x), produciendo un resto.
3. Transmite $T(x) = x^rM(x)$ - *resto*. T(x) es divisible por G(x). Sus últimos r bits son el checksum.

Si hay errores en la transmisión recibiremos T(x)+E(x) en vez de T(x). El receptor divide T(x)+E(x) por G(x). Ya que el resto debido a T(x) es 0, el resto obtenido es completamente debido a E(x). Si E(x) tiene G(x) como un factor, el resto será 0 y no detectaremos el error, de otro modo, sí. Si hay un error de un bit, $E(x) = x^i$. Si G(x) tiene más de un término, no puede dividir E(x). Entonces, podemos detectar todos los errores de un bit. Con dos errores tendremos $E(x) = x^i + x^j = x^j (x^{i-j} + 1)$. Podemos usar un G(x) que no divide $x^k + 1$ para cualquier k hasta el valor máximo de i-j (que es la longitud del marco). Por ejemplo, $x^{15} + x^{14} + 1$ no divide $x^k + 1$ para $k < 32768$. Si x+1 es un factor de G(x), podemos detectar todos los errores que consisten en un número impar de bits invertidos. Prueba por contradicción: Asume que E(x) tiene un número impar de términos y es divisible por x + 1. Entonces $E(x) = (x + 1)Q(x)$ por algún Q(x). $E(1) = (1 + 1)Q(1) = (0)Q(1) = 0$. Pero E(1) debe ser 1 porque consiste en la suma de un número impar de 1's.
Podemos detectar todos los errores en grupo con longitudes menos de o igual a r. Si el grupo tiene una longitud de k, lo podemos escribir como $x^i (x^{k-1} +...+ 1)$ (i ubica el grupo en el marco). Si G(x) contiene un término de x^0, x^i no puede ser un factor y G(x) no puede ser igual a $x^{k-1} +...+ 1$ (el grado k-1 es menos de r). Si el grupo tiene una longitud de r + 1, la probabilidad que el grupo es G(x) es la probabilidad que los r - 1 bits intermedios del grupo son iguales (por definición el primer y el último bits del grupo son 1), que es $(1/2)^{r-1}$. Para los grupos con longitudes mayor de r + 1, la probabilidad es $(1/2)^r$.

Como Normas Internacionales tenemos las siguientes:

$$CRC\text{-}12 = x^{12} + x^{11} + x^3 + x^2 + x + 1$$
$$CRC\text{-}16 = x^{16} + x^{15} + x^2 + 1$$
$$CRC\text{-}CCITT = x^{16} + x^{12} + x^5 + 1$$

Los dos últimos detectan todos los errores de uno y dos bits, los errores con un número impar de bits invertidos, los grupos de errores con longitudes menos de o igual a 16, 99,997% con longitudes de 17, y 99,998% con longitudes mayor o igual a 18.

1.1.1.3 Capa de Red

Se encarga de suministrar una conexión de extremo a extremo, es decir, la transmisión de información entre sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores (les proporciona independencia) de preocuparse por las tecnologías de conmutación utilizadas para conectar los sistemas.

Las funciones de mayor importancia de la capa de red son:

- Direccionamiento Lógico.
- Esta capa mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.
- Realiza control de congestión.
- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Enrutamiento de paquetes.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como paquetes.
- La capa de red proporciona los medios para establecer, mantener y terminar las conexiones de red; proporciona los medios funcionales y procedimientos para el intercambio de información entre las entidades de transporte sobre las conexiones de la red.
- Proporciona a las entidades de transporte independencia con respecto al enrutamiento y a las consideraciones de transmisión asociadas con el establecimiento y la operación de una conexión de red dada.

Algunos de los protocolos que funcionan en la capa de red son: Internet Protocol (IP) y Internetwork Packet eXchange (IPX).

1.1.1.4 Capa de Transporte

Controla la interacción entre procesos usuarios, incluye controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones, controla el flujo de transacciones y direccionamiento de máquinas a procesos de usuario. Esta capa asegura que se reciban todos los datos y en el orden adecuado, provee un transito confiable de datos a través de la capa de red realizando un control de extremo a extremo. Algunas de las funciones realizadas son:

- Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red.
- Multiplexaje.
- Regula el control de flujo del tráfico de extremo a extremo.
- Reconoce los paquetes duplicados.

- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario (puntos extremos de una conexión).
- Provee la función de difusión de mensajes (broadcast) a múltiples destinos.
- Detección y corrección de errores.
- Entrega confiable de paquetes.
- Administración de circuitos virtuales.

Ejemplos de protocolos que trabajan en esta capa son: Transmission Control Protocol (TCP), User Datagram Protocol (UDP) y Sequenced Packet Exchange (SPX).

1.1.1.5 Capa de Sesión

Normaliza el proceso de establecimiento, administración y terminación de una sesión. Si por algún motivo esta sesión falla esta restaura la sesión sin perdida de datos, o si esto no es posible termina la sesión de una manera ordenada, checando y recuperando todas sus funciones. Establece las reglas o protocolos para el diálogo entre máquinas y así poder regular quien habla y por cuanto tiempo, o si hablan en forma alterna, es decir, las reglas del diálogo que son acordadas. Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos. Algunas de las funciones que realiza son las siguientes:

- Establecimiento de la conexión de sesión.
- Intercambio de datos.
- Liberación de la conexión de sesión.
- Sincronización de la sesión.
- Administración de la sesión.
- Permite a usuarios en diferentes máquinas establecer una sesión.
- Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.
- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Función de sincronización.

1.1.1.6 Capa de Presentación

Sus funciones están relacionadas con el conjunto de caracteres o códigos de datos que son usados, o la manera como van a ser presentados en pantalla o como van a ser impresos, cuando un conjunto de caracteres llega a una pantalla, se dan ciertas acciones para una presentación correcta de la información. Esta capa también tiene que ver con el conjunto de caracteres que debe presentar una edición de datos, salto de línea, colocación de datos en columnas, adición de encabezados fijos para las columnas, etc. La capa de presentación cubre dos aspectos complementarios:

1. La representación de los datos a ser transferida entre entidades de presentación, y
2. La representación de la estructura de datos a la cual entidades de aplicación hacen referencia en a lo largo de su comunicación en conjunto con la

representación del conjunto de acciones que pueden ser aplicadas a las estructuras de datos manejados.

En esta capa se realizan las siguientes funciones:

- Se da formato a la información para visualizarla o imprimirla.
- Se interpretan los códigos que estén en los datos (conversión de código).
- Se gestiona la encriptación de datos.
- Se realiza la compresión de datos.
- Establece una sintaxis y semántica de la información transmitida.
- Se define la estructura de los datos a transmitir (define los campos de un registro: nombre, dirección, teléfono, etc.).
- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).
- Compresión de datos.
- Criptografía

A la capa de presentación le atañe la sintaxis pero no la semántica.

1.1.1.7 Capa de Aplicación

Provee los medios necesarios a los procesos de aplicación para acceder al ambiente OSI, siendo la capa más alta en el modelo de referencia. Aquí se ubica la interfaz de las aplicaciones con los usuarios finales del sistema.

Relacionado con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema. Por ejemplo, control de transferencia de archivos, soporte al operador funciones de dialogo de alto nivel, actividades de bases de datos de alto nivel. Los tres primeros niveles proporcionan una variedad de servicios que son empleados en la sesión de los usuarios, a este subconjunto se le denomina subsistema de la sesión de servicios. Se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las cuales gestionan:

- Transferencia de archivos (FTP).
- Intercambio de mensajes (correo electrónico).
- Acceso remoto (rlogin, telnet).
- Acceso a bases de datos, etc.

1.2 Redes de Área Local LAN

1.2.1 Tecnologías en Redes de Área Local

1.2.1.1 Ethernet

En 1972, Xerox Corporation desarrolló el primer sistema Ethernet experimental, utilizando cable coaxial como medio físico de transmisión y con una tasa de transferencia de 2.94 Mbps. Gracias a estos logros Xerox Corporation introdujo en 1975 el primer producto Ethernet. El Ethernet de Xerox fue tan exitoso que el consorcio Digital, Intel y Xerox (DIX)

crearon una norma para Ethernet de 10 Mbps, la primera versión de Ethernet. En 1982 es liberada la versión 2 y se inicia en el mismo año su normalización por parte de la IEEE. El diseño de Ethernet de 10 Mbps fue la base de la especificación ANSI/IEEE 802.3, publicada y liberada oficialmente en el año de 1985, ya antes había sido aprobada por el grupo de trabajo 802.3 en 1983. En éste mismo año, Novell NetWare libera un formato de trama propietario basado en la norma preliminar de 802.3. Dos años después la versión final de 802.3 (1985) es liberada, incluyendo el encabezado LLC, haciendo la tramade Novell Netware incompatible con el definido por la IEEE. Finalmente, el formato 802.3 SNAP fue creado para permitir la compatibilidad entre la versión 2 de Ethernet y el 802.3.

1.2.1.1.1 Elementos de la Red Ethernet

Una Red Local basada en la norma 802.3 esta compuesta básicamente de nodos de red y un medio de interconexión. Los nodos de red son de dos tipos principalmente:

- *Equipo terminal de Datos (Data Terminal Equipment, DTE):* Son dispositivos que pueden ser usados con dos propósitos diferentes; como fuentes o como destino de las tramas de datos que se circulan en la red. Los equipos terminales son usualmente PCs, Workstations, Servidores de archivos o Servidores de impresión.
- *Equipo de Comunicación de Datos (Data Communication Equipment, DCE):* Son dispositivos de red que reciben y reenvían las tramas a través de la red. Los Repetidores, Switches y Enrutadores, son ejemplos de equipos de comunicación de datos y entran en la categoría de dispositivos “standalone” (una vez configurado, el equipo realiza solo los procesos); en cambio las tarjetas de interfaz de red y los módems son equipos de comunicación de datos y caen dentro de la categoría unidades de interfaz de comunicación.

1.2.1.1.2 Topologías de la Red Ethernet

En una red del tipo Ethernet, la transmisión realizada por un dispositivo es “escuchada” por todos los demás dispositivos conectados a la LAN, teniéndose que la topología lógica es del tipo BUS, cada estación está ligada en "paralelo" al bus (Figura 4). Cada host escucha los paquetes y si la dirección destino es la propia lo recibe y procesa, si no es para él lo descarta. Esta topología se implementó físicamente usando cable coaxial como medio de transmisión; sin embargo, en la práctica actual es común usar topología física de estrella (Figura 5), si bien a nivel lógico siguen siendo un bus. Para facilitar su implementación se hace uso del par trenzado como medio de transmisión donde los dispositivos son concentrados a un concentrador o switch, que funcionan como un punto común de conexión en paralelo al bus. Si bien lo visto corresponde a una topología en estrella, es extensivo al uso de varios concentradores o switches ligados entre si en un formato jerárquico, como una topología física de árbol, a veces se denomina estrella jerárquica. Debe recalcarse que la topología lógica sigue siendo un bus en todos los casos.

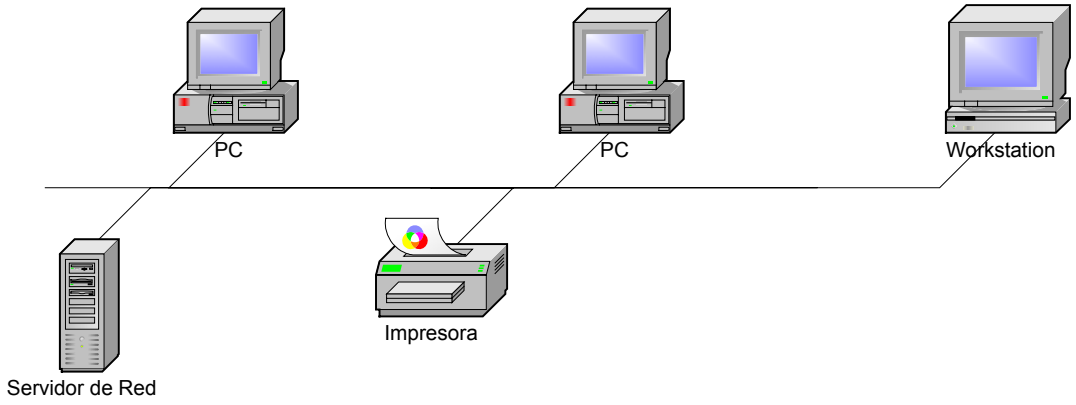


Figura 4. Topología de Bus.

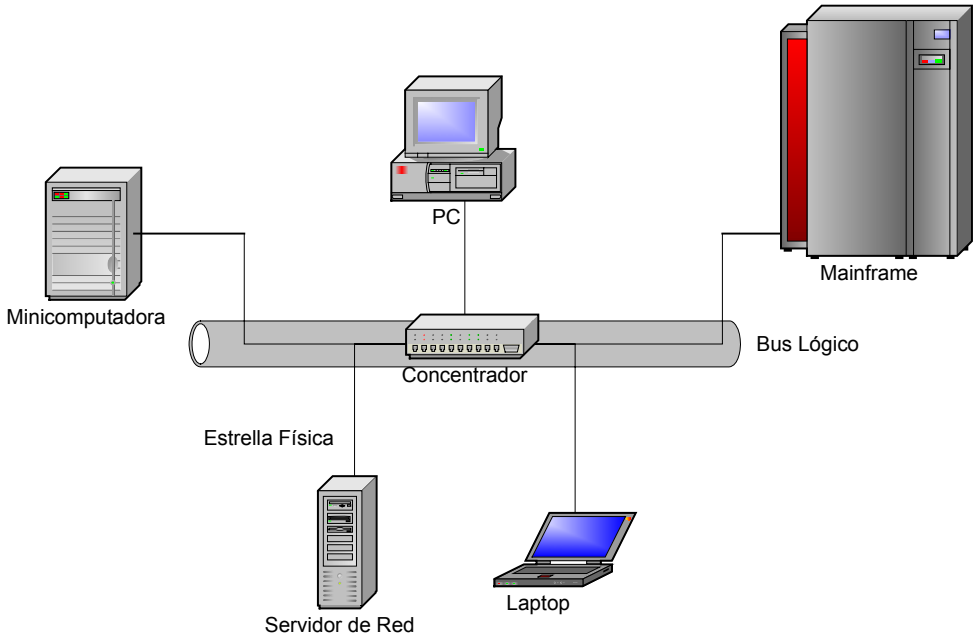


Figura 5. Topología de Estrella.

1.2.1.1.3 Técnica de Acceso al Medio: CSMA/CD

El CSMA/CD funciona de la siguiente manera:

Cuando un host desea mandar información primero escucha el cable de la red para revisar que no se este usando en ese preciso momento (Carrier-Sense). Esta es una técnica de acceso al medio por contención; esto se oye muy sencillo, pero el problema reside en que dos o más hosts al censar que no se esta usando el medio, pueden mandar al mismo momento su información (Multiple Access), y como solamente puede haber uno y sólo un mensaje en tránsito en el medio se produce una colisión. Entonces, los hosts detectan la colisión y reenvían su información en un intervalo aleatorio, es importante que sea aleatorio ya que si ambos hosts tuvieran el mismo intervalo se producirá un ciclo

vicioso de colisiones y reenvíos (Collision Detection). Así por ejemplo, al detectar la colisión un host se espera tres milisegundos y el otro cinco milisegundos, siendo obvio que un host reenviara su información primero y el otro esperará a que el medio este libre.

En pocas palabras, un nodo que desea transmitir espera a que el medio esté desocupado, una vez que se encuentra en este estado empieza la transmisión. Si otro nodo empezara también a transmitir en este instante se producirá una colisión, por lo tanto se detiene la transmisión y se retransmite tras un retraso aleatorio. Evidentemente que en una misma red Ethernet al haber muchos hosts tratando de enviar datos al mismo tiempo y/o al haber una transferencia masiva de datos se crea un gran porcentaje de colisiones y utilización de la red. Si se pasa del 1% de colisiones y/o 40% de utilización del medio, se dice que la red está saturada.

Si un host tiene información que transmitir:

1. Censa el medio para asegurar que nadie esté transmitiendo, es decir, verifica que el medio de transmisión esté libre para su uso, en este momento no existe señal alguna sobre el medio de transmisión.
2. Transmite la información.
3. Si el medio está ocupado, esperará hasta que esté libre.
4. Si ocurre que dos hosts comienzan a transmitir al mismo tiempo, se produce una colisión, la cual es detectada por varios hosts como una variación inusual de voltaje. Detectada la colisión, se interrumpe inmediatamente la transmisión dla tramay se transmite una señal “jam” (32 bits, comúnmente sólo unos) mientras se espera un tiempo aleatorio para volver intentar acceder al medio.

Es importante recalcar que existen dos tipos de colisiones. La colisión temprana es la que ocurre normalmente en una red Ethernet bien dimensionada y es aquella colisión que sucede antes de haberse transmitido 512 bits en el medio, lo cual permite que los hosts involucrados en la colisión la detecten y puedan retransmitir la información en proceso de transmisión (Figura 6). Por su parte una colisión tardía ocurre después de haberse transmitido 512 bits en el medio, lo cual no permite que todos los hosts involucrados en una colisión se enteren que su información recién transmitida fue dañada y que por lo tanto se requiere su retransmisión (Figura 7).

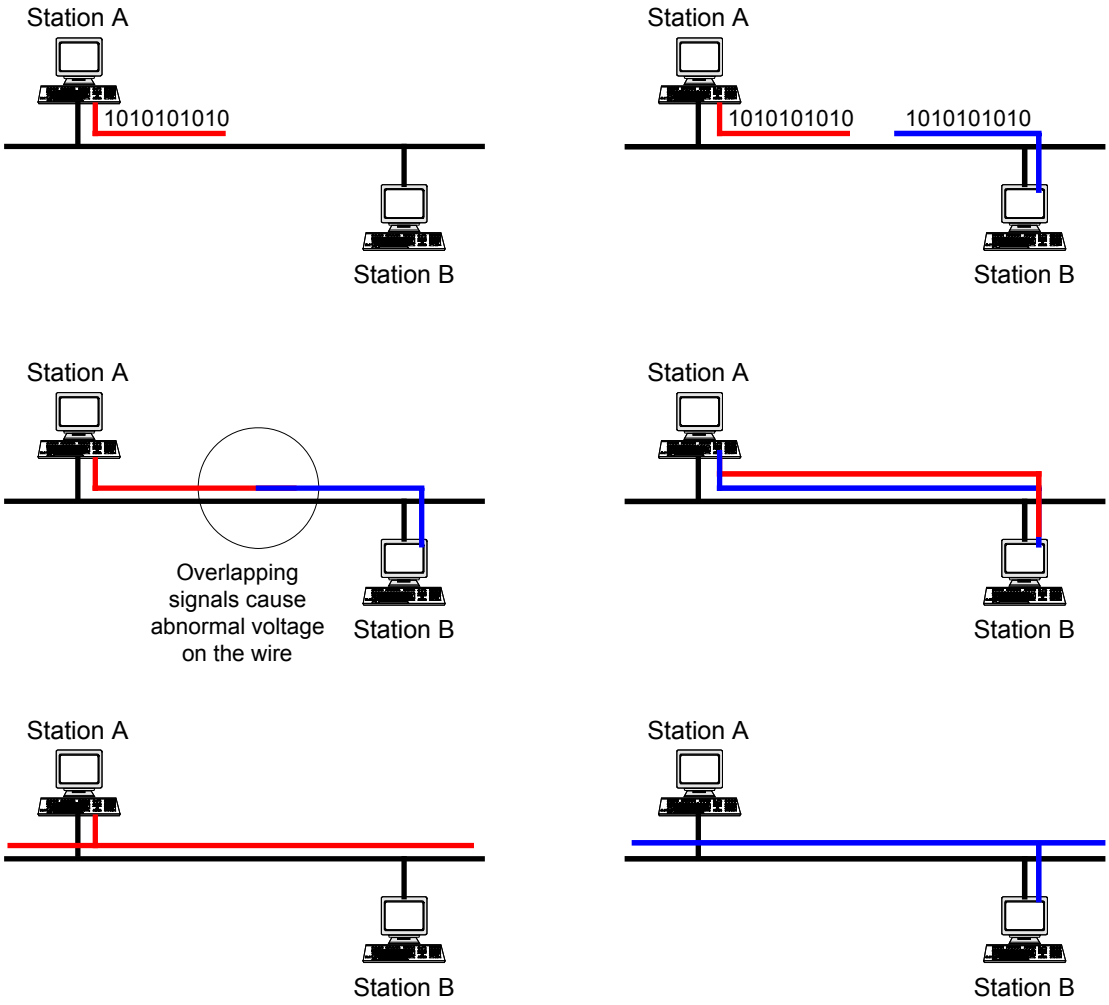


Figura 6. Secuencia de una colisión temprana.

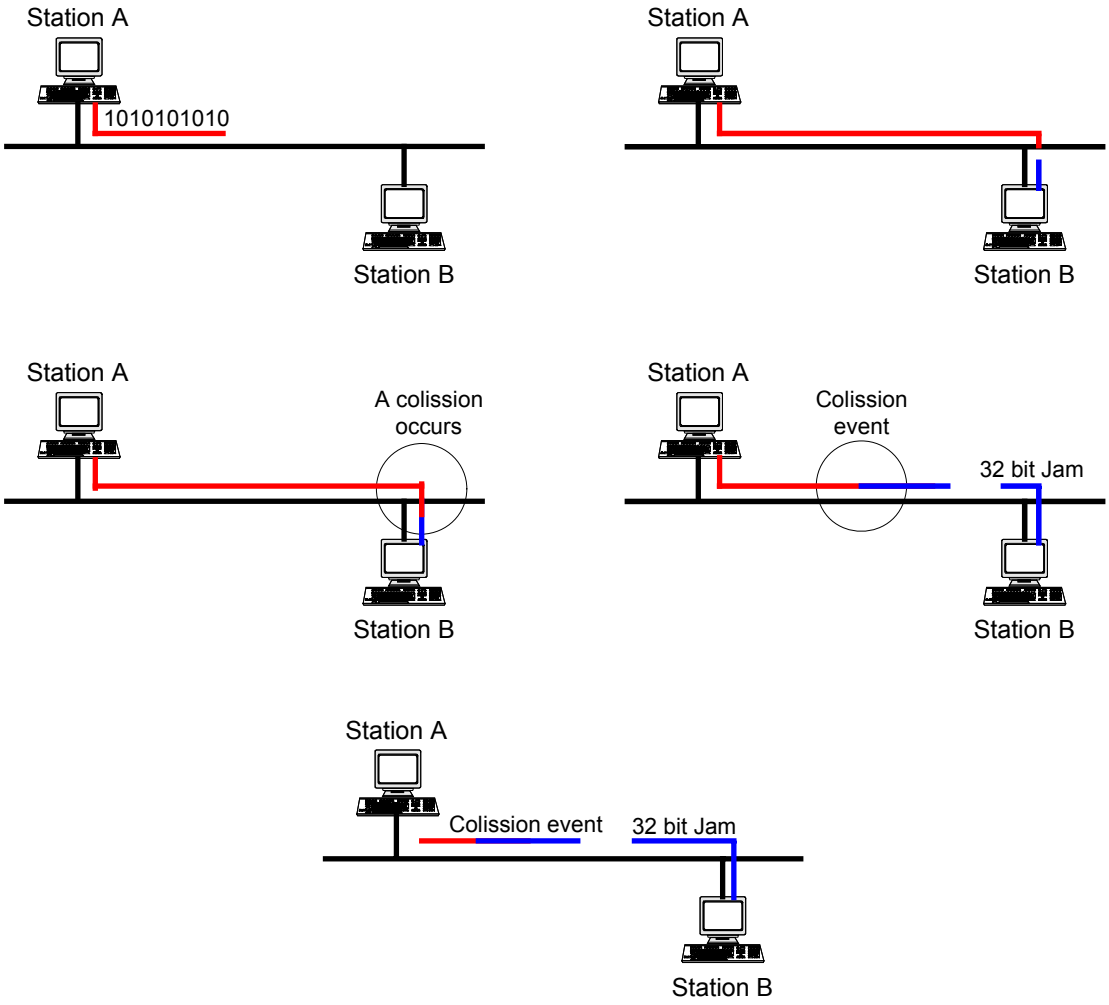


Figura 7. Secuencia de una colisión tardía.

1.2.1.1.4 Formato de Trama Ethernet

La norma IEEE 802.3 define el formato básico de trama de datos, el cual es requerido por todas las implementaciones MAC, además, muchos formatos opcionales pueden ser usados para extender la capacidad básica de protocolos. El formato básico de trama de datos contiene siete campos (Figura 8):

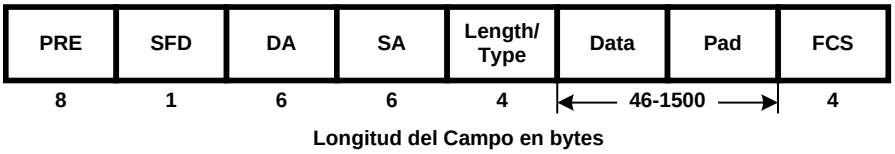


Figura 8. Formato Básico de Trama Ethernet.

1.2.1.1.4.1 Campos

Preamble (PRE): Consta de 7 bytes. El PRE es un patrón alternativo de unos y ceros que le dice a los hosts receptores que un trama esta llegando, y esto provee un medio para sincronizar la porción de las tramas recibidos desde la capa física de la cadena de bits entrantes.

Start of trama delimiter (SFD): Consta de 1 byte. El SFD es un patrón alternativo de unos y ceros, que terminan con dos bits en uno consecutivos, indicando que el siguiente bit es el bit más significativo del campo de la dirección destino.

Destination Address (DA): Consta de 6 bytes. El campo de DA identifica cual es leal host que debe recibir el trama. El bit más significativo del campo DA indica si la dirección es individual o unicast (cuando el bit es cero) o si se trata de una dirección de grupo o multicast (cuando el bit es uno). El segundo bit más significativo significa si el DA es administrado globalmente (cuando el bit es cero) o es localmente administrado (cuando el bit es uno). Los restantes 46 bits son un valor único asignado que define un único host, un grupo de hosts o todos los hosts en la red.

Source Address (SA): Consta de 6 bytes. El SA identifica el host transmisor. El SA siempre es una dirección individual y el bit más significativo de este campo siempre es cero.

Length/Type: Consta de 4 bytes. 2 bytes proporcionan la longitud del campo Data y 2 bytes que identifican a qué protocolo de la capa superior va dirigida la información. Si el valor del campo de Length/Type es menor o igual a 1500, el número de bytes del LLC en el campo de datos es igual al valor del campo Length/Type. Si el valor del campo Legth/Type es mayor que 1536 la tramaes un trama de tipo opcional y el valor del campo Length/Type identifica el tipo particular dla tramaque se envío o recibío.

Data: De 46 a 1500 bytes, contiene la información destinada a capas superiores. Es una secuencia de N bytes de algún valor, donde N es menor o igual a 1500 bytes, si la longitud del campo de datos es menor que 46 bytes, el campo de datos debe ser rellenado adicionándole bytes hasta que tenga longitud de 46 bytes. Si es mayor de 1500 bytes se dice que la tramaes un *giantgiant*, ya que el valor definido para el MTU para Ethernet es de 1500 bytes.

Trama Check Sequence (FCS): Consta de 4 bytes. Esta secuencia contiene un valor de un ciclo redundante de chequeo (CRC) de 32 bits, el cual es creado por la MAC transmisora y es recalculado por la MAC receptora para verificar si la tramaestá dañado. El FCS es generado con los campos DA, SA, Length/Type y el de datos.

Existen cuatro tipos de trama para Ethernet y son los siguientes: Ethernet versión 2, 802.3, Novell y SNAP. Todos tienen una longitud mínima de 64 bytes y una máxima de 1518 bytes (sin contar el campo preámbulo).

1.2.1.1.4.2 Trama Ethernet Versión 2

Esta trama posee los siguientes campos:

Preamble: Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en “11”. La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

Type: 2 bytes que identifican a qué protocolo de la capa superior va dirigida la información.

Data: De 46 a 1500 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Type y Data. La máquina receptora genera este código cuando recibe la tramay lo compara con el que recibe. Si los dos tramas son iguales la información está correcta, si son diferentes, la información contiene errores y la tramaes descartado.

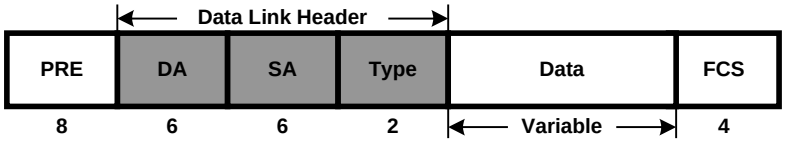


Figura 9. Formato de Trama Ethernet versión 2.

1.2.1.1.4.3 Trama Ethernet Novell Raw

Este trama consiste de los siguientes campos:

Preamble: Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en “11”. La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

Lenght: 2 bytes que proporcionan la longitud del campo Data.

IPX Header: 2 bytes nunca usados y puestos en FFFF.

Data: De 44 a 1498 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Length, los dos bytes en "FF" y Data. La máquina receptora genera este código cuando recibe la tramay lo compara con el que recibe. Si son iguales la información está correcta, si son diferentes, la información tiene errores y la tramaes descartado.

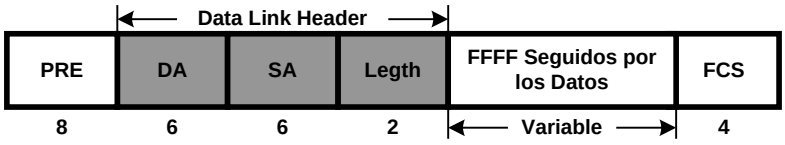


Figura 10. Formato de Trama Ethernet Novell Raw.

1.2.1.1.4.4 Trama Ethernet 802.3

Este trama tiene los siguientes campos:

Preamble: Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11". La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

Lenght: 2 bytes que proporcionan la longitud del campo Data.

LLC Header: 3 bytes de header LLC o 802.2

Data: De 43 a 1497 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Length, LLC y Data. La máquina receptora genera este código cuando recibe la tramay lo compara con el que recibe. Si son iguales la información está correcta, si son diferentes, la información tiene errores y la tramaes descartado.

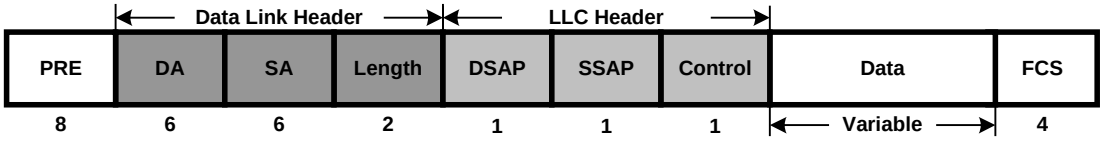


Figura 11. Formato de Trama Ethernet 802.3.

1.2.1.1.4.5 Trama Ethernet SNAP

Este trama consiste de los siguientes campos:

Preamble: Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11". La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

Lenght: 2 bytes que proporcionan la longitud del campo Data.

LLC Header: 3 ó 4 bytes de header LLC o 802.2. DSAP y SSAP están puestos cada uno en AA hexadecimal, el byte de control identifica el tipo de trama LLC y usualmente tiene el valor de 03 hexadecimal.

Snap Header: 5 bytes

> *Vendor Code:* 3 bytes de código de operador, usualmente iguales a los primeros 3 bytes del DA, en otro caso son puestos en 0.
>
> *Local Code:* 2 bytes que contienen usualmente la misma información que el campo Type en Ethernet Versión 2.

Data: De 38 a 1492 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Length, LCC, SNAP y Data. La máquina receptora genera este código cuando recibe la tramay lo compara con el que recibe. Si son iguales, la información está correcta, si son diferentes, la información tiene errores y la tramaes descartado.

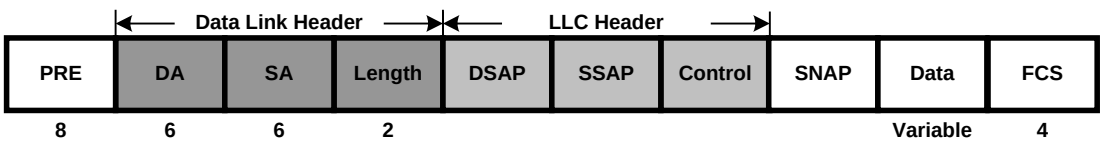


Figura 12. Formato de Trama Ethernet SNAP.

1.2.1.1.4.6 Logical link Header (802.2)

La idea de este header LLC (Figura 13) es el de proveer de más información a las capas superiores indicando en qué buffer de memoria se coloca la información recibida por la tarjeta.

DSAP (Destination Service Access Point): Este campo corresponde a un puntero en el buffer de memoria del host receptor del paquete, el cual, es utilizado por la "tarjeta receptora" para saber en cual buffer colocar esta información. Esto es particularmente útil en situaciones donde un usuario está usando múltiples protocolos. En el caso de ser un paquete del tipo IEEE 802.3 SNAP, este campo contiene el valor 0xAA.
SSAP (Source Service Access Point): Este campo es análogo al DSAP, pero se refiere al host emisor. En el caso de ser un paquete del tipo IEEE 802.3 SNAP, este campo contiene el valor 0xAA.
Control Byte: Este byte indica el tipo de LLC (Logical Link Header).

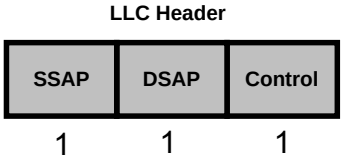


Figura 13. Formato dla tramaLLC Header.

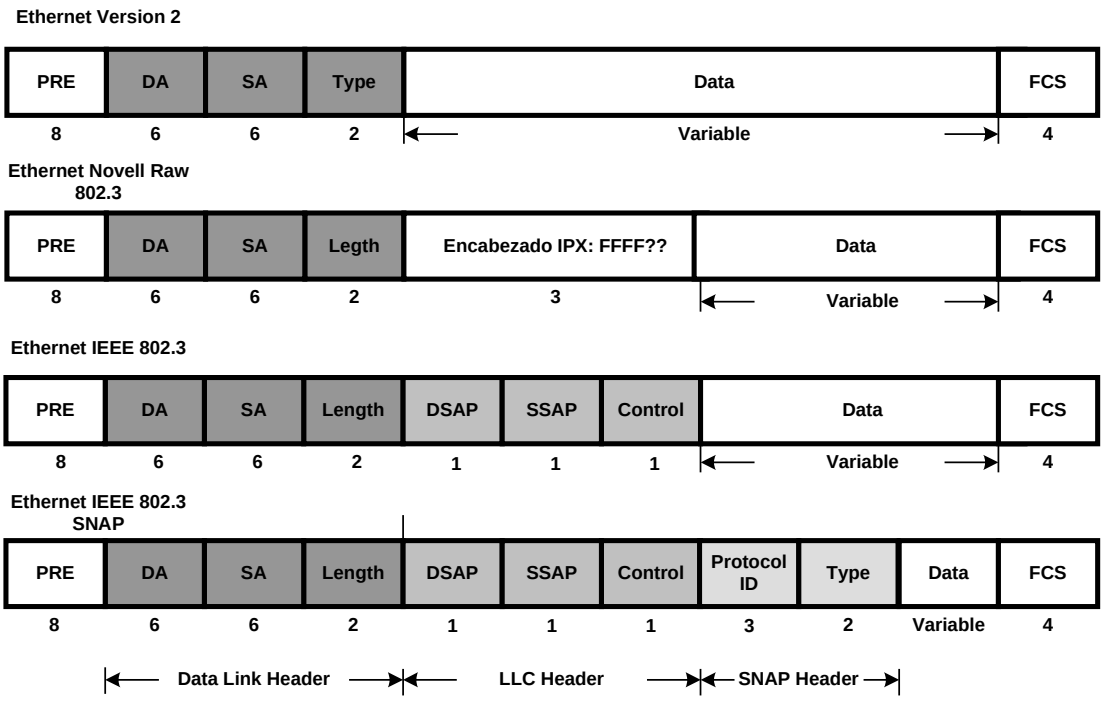


Figura 14. Comparación de los distintos formatos de Trama Ethernet.

1.2.1.1.5 Implementaciones Físicas

La norma 802.3 define cuatro tipos de implementación física para Ethernet:

1.2.1.1.5.1 10Base-T

Esta es una especificación técnica que se utiliza en redes Ethernet. 10BASE-T forma parte de la especificación del organismo de normas IEEE para Ethernet (10Mbps) sobre las categorías 3, 4 o 5 de cable UTP (dos pares de cables - un par para transmitir datos y el segundo para recibirlos). 10BASE-T tiene un límite de distancia por segmento de 100m (328 pies) aproximadamente, conector ISO 8877: RJ-45.

1.2.1.1.5.2 10Base-2

10BASE2 forma parte de la especificación del organismo de normas IEEE para Ethernet 10Mbps, y es un cable coaxial delgado, también conocido como *thinnet* o *cheapernet*. 10BASE2 tiene un límite de distancia por segmento de 185m aproximadamente (607 pies).

1.2.1.1.5.3 10Base-5

Esta es una especificación técnica utilizada en las redes Ethernet. 10BASE5 forma parte de la especificación del conjunto de normas IEEE para Ethernet 10Mbps, y es un cable coaxial grueso, también conocido como *thicknet*. 10BASE5 tiene una distancia límite por segmento de 500m (1640 pies) aproximadamente, utiliza cable coaxial de 50 ohms y conectores AUI, con topología de bus.

1.2.1.1.5.4 10Base-FL

Forma parte de la especificación del conjunto de normas IEEE para utilizar cable de fibra óptica de 10Mbps (Ethernet). Los segmentos de una red que utilizan cables de 10 BASE-FL pueden ser de hasta 2km (1.24 millas) de longitud.

1.2.1.2 Fast Ethernet

El crecimiento de las redes de área local ha sido conducido a través de la introducción de la tecnología Ethernet, al igual que los dispositivos de red disponibles en el mercado. Como resultado de lo anterior, muchas aplicaciones pueden correr ahora en una red LAN. Pero algunas aplicaciones de multimedia como: streaming, videoconferencia o VoIP pueden provocar que las redes se vuelvan más lentas, cuando se trata de redes que utilizan 10 Mbps, como en Ethernet.

La velocidad de las redes y su disponibilidad son requerimientos críticos. Con más aplicaciones que requieren mayores velocidades en una LAN para tener un desempeño

aceptable, los administradores de redes se enfrentan a una gran cantidad de opciones para implementar tecnologías de alta velocidad para una LAN.

La especificación final del 802.3u fue aprobada en Junio de 1995. Dentro de otros objetivos de esta alianza se tiene:

- Mantener el CSMA/CD (Carrier Sense Multiple Access Collision Detection).
- Soportar los esquemas populares de cableado (Por ejemplo: 10BaseT).
- Asegurar que la tecnología Fast Ethernet no requerirá cambios en los protocolos de las capas superiores, ni en el software que corre en los hosts de trabajo LAN. (por ejemplo, no se necesita realizar cambios para el software de SNMP, ni para las MIBs.

El objetivo principal de la alianza es el de asegurar que se pueda pasar del Ethernet tradicional a Fast Ethernet, manteniendo el protocolo tradicional de transmisión de Ethernet.

Fast Ethernet surge utilizando la misma topología lógica y física, con el mismo formato de trama y la misma técnica de acceso al medio que Ethernet. Además, de la tasa de transmisión tiene algunas diferencias como la autonegociación y el uso opcional de fibra óptica como medio de transmisión.

1.2.1.2.1 Implementaciones Físicas

La recomendación 802.3u define tres tipos de implementación física para Fast Ethernet.

1.2.1.2.1.1 100Base-T4

Cuatro pares de UTP Categoría 3, 4 y 5. Los datos son transmitidos en 3 pares (cada uno a 33 Mbps) utilizando codificación 8B/6T, la cual permite frecuencias menores y un decremento de las emisiones electromagnéticas, y el cuarto par es para detectar colisiones. El sistema de comunicación es half-duplex, debido a que utiliza 3 pares para transmitir y recibir.

1.2.1.2.1.2 100Base-TX

Dos pares de UTP categoría 5 o STP Tipo I half duplex. Un par para transmisiones (con una frecuencia de operación de 125 MHz a 80% de eficiencia para permitir codificación 4B5B). Y el otro par para detectar colisiones y recibir. Utiliza un esquema de codificación MLT-3, también utilizado en ATM. El sistema de comunicación es half o full-duplex. La longitud máxima de los segmentos es de 100m, con una topología de estrella y usa conectores RJ-45.

1.2.1.2.1.3 100Base-FX

Fibra óptica de 62.5/125 - micron multimodo. Capaz de sostener un throughput de 100 Mbps en distancias mayores a 100m. Utiliza una fibra para transmisiones y la otra para detección de colisiones y para recibir. El sistema de comunicaciones es half o full-duplex.

La distancia máxima del segmento es de 400m, con una topología punto a punto, utiliza conectores MIC (*Duplex media Interface Connector*) ST.

1.2.1.2.2 Autonegociación

La autonegociación es una característica opcional que habilita el intercambio de información entre dos hosts de acuerdo con sus recursos, ya sea a 10 Mbps o a 100 Mbps. La autonegociación es ejecutada mediante el paso de información encapsulada en un tren de pulsos, éstos son los mismos usados por 10baseT para verificar la integridad del enlace. Si una estación tiene un pulso sencillo, referido como NLP (*Normal Link Pulse*), ésta reconoce que el dispositivo en la otra punta sólo es capaz de manejar 10baseT. Si la autonegociación esta siendo usada por una estación, ésta transmitirá un tren de pulsos referidos como FLP (*Fast Link Pulse*). Un FLP consiste de 17 pulsos de reloj inter-espaciados con 16 pulsos de señal para formar una palabra código de 16 bits. Si un pulso de señal ocurre entre dos pulsos de reloj, tal bit es 1, si no ocurre pulso de señal, tal bit es cero. La palabra código de 16 bits describe qué implementación de Ethernet es soportada, de tal forma que los hosts en autonegociación (regularmente un host final y un concentrador o un switch) seleccionen cual implementación se usará de acuerdo con las siguientes prioridades:

100BASE-TX full duplex
100BASE-T4
100BASE-TX
10BASE-T full duplex
10BASE-T

La palabra código de 16 bits consta de los siguientes campos:

Selector field (5bits)
Tecnology abalibity field (8 bits)
Remote fault bit
Acknowledge bit
Next page bit

1.2.1.3 Gigabit Ethernet

Los servidores actuales están diseñados para procesar archivos de mayor tamaño y para mover los datos más rápido que nunca. Pero cuando las redes no se han diseñado para admitir niveles equivalentes de rendimiento, se arriesga la disponibilidad y se reducen el rendimiento y el ancho de banda. Los resultados que los usuarios de la red aprecian son un servicio lento y errores de datos. Dos factores contribuyen significativamente a la carga cada vez mayor de las redes locales:

Más usuarios finales con conexiones de 100 Mbps:

- Los nuevos hosts están equipados para velocidades de 100 Mbps.
- Las nuevas y potentes aplicaciones para equipos desktop, para multimedia, tratamiento de imágenes y gestión empresarial, están consumiendo el ancho de banda.

- Los usuarios exigen más de la red y crean la necesidad de una tecnología aún más potente en la propia red.

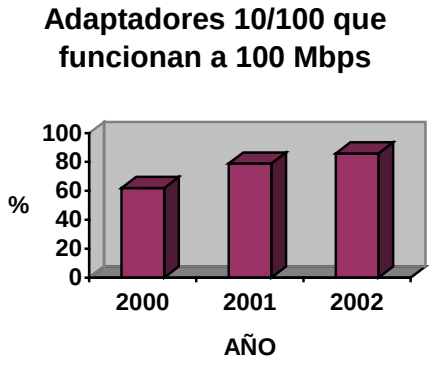


Figura 15. Tendencias en Velocidad de Equipos Desktop.

El cambio de papel de la Red:

- Las Intranet son algo común y generan unos niveles sin precedentes de uso compartido de datos.
- Las organizaciones con varios centros confían en las redes para acceder a sus datos centralizados.
- Las extranet soportan volúmenes enormes de tráfico a destinos fuera de la red local.
- Los negocios electrónicos generan un intercambio intensivo de datos, lo que exige una seguridad y una calidad de servicio especializados.

Ethernet, con 20 años de antigüedad, es la tecnología de facto para la conexión entre redes. La plataforma ha proporcionado una auténtica escalabilidad a lo largo del tiempo. El salto de Ethernet (10 Mbps) a Fast Ethernet (100 Mbps) permitió a los usuarios trabajar con volúmenes superiores de datos y con aplicaciones cada vez más sofisticadas. La llegada de Gigabit Ethernet (1000 Mbps) ofrece aún más ventajas.

En junio de 1998, la IEEE aprobó una norma Gigabit Ethernet sobre cable de fibra óptica, 1000BASE-X (IEEE 802.3z). Con la aprobación de 802.3z, las empresas podían hacer uso de una tecnología probada y normalizada para mejorar el flujo de tráfico en áreas de red congestionadas. No obstante, la creación de una red de cable de fibra óptica presenta sus problemas. Tener que volver a cablear un edificio es difícil y, por lo tanto, caro. Las ventajas de Gigabit Ethernet quedaron fuera del alcance de la mayoría de las empresas por sus costos.

En junio de 1999, la IEEE aprobó 802.3ab, una nueva norma para Gigabit Ethernet sobre cobre, una tecnología conocida como 1000BASE-T. Hoy en día, las redes pueden proporcionar velocidad Gigabit sobre la infraestructura de cobre existente, con lo que se reducen, e incluso se eliminan, los costos asociados con el tendido de cable de fibra óptica.

1.2.1.3.1 Implementaciones Físicas

1.2.1.3.1.1 1000Base-X

Gigabit Ethernet se diseñó originalmente como una tecnología conmutada, y se utilizaba cable de fibra óptica para los enlaces ascendentes y para las conexiones entre edificios. La fibra se utilizaba habitualmente para conectar instalaciones de red en zonas amplias; las normas IEEE especifican fibra para tramos de cableado de más de 100 metros. Incluso cuando no se trata de grandes distancias, el entorno puede desempeñar un papel en la elección de fibra o cobre. Por ejemplo, la fibra es inmune a las interferencias electromagnéticas que pueden afectar a los archivos transmitidos por cable de cobre. Para distancias de cableado de estructuras principales de 300 a 550 metros, se recomienda la solución de fibra multimodo. Para tendidos verticales, la mejor opción puede ser una combinación de producto en unimodo y en varios modos, con una fibra de varios modos de ancho de banda superior.

La fibra puede ser la mejor opción para aplicaciones dentro del edificio y las situaciones en que el tendido de cableado tiene que estar al descubierto. El cable de fibra óptica no puede partirse, excepto en salas limpias, lo que hace prácticamente imposible que los piratas informáticos lo manipulen.

1.2.1.3.1.2 1000base-T

Con la tecnología 1000BASE-T, los diseñadores de redes pueden ofrecer rendimiento Gigabit en toda la red mediante el cable de cobre categoría 5 que ya existía. La parte de ingeniería de red ahora tiene la libertad de elegir el tipo de cable (fibra o cobre) que sea más conveniente para cada segmento de red. La instalación de cable de fibra óptica puede ser difícil, y por lo tanto, más costosa que la de cable de cobre. La terminación y los conectores, así como los transceivers ópticos para fibra unimodo, son más caros que para fibra multimodo. En general, a menos que preocupe la seguridad o las interferencias, no existe una razón empresarial poderosa para desplegar fibra hasta un host. Si se lleva fibra al puesto de trabajo, habrá que sustituir los puertos del switch tres o cuatro veces a lo largo de la vida útil de la planta de cableado. También se debe tener en cuenta que la tecnología de fibra actual no puede proporcionar alimentación a los dispositivos conectados a la red a nivel de puesto de trabajo, es decir: teléfono de red local, teléfonos IP, cámaras Web. 1000BASE-T admite las mejores prestaciones de Fast Ethernet y ofrece un entorno fiable para las prestaciones avanzadas de Gigabit Ethernet, como calidad de servicio, alto nivel de seguridad y aplicación de las políticas. Siempre que funcione Fast Ethernet, se pueden aplicar fácilmente las soluciones 1000BASE-T. Es una transición sencilla y económica que puede reducir con rapidez los cuellos de botella en las conexiones a servidor, en las colas de los switches y en otros puntos de incorporaciones.

1.2.1.3.2 Preparación para 10Gbps

Las normas Ethernet han evolucionado con rapidez, y cada avance se ha apoyado en las normas anteriores, ofreciendo así una vía de compatibilidad con lo que ya existía. Esta compatibilidad hace que la tecnología Gigabit sea fácil de escalar. Distintos dispositivos de conectividad 10/100/1000 permiten a los responsables poner a punto la velocidad de la

red para determinados grupos o segmentos de trabajo, mientras que otros podrán migrar en un futuro a velocidad Gigabit. Esta vía de migración es coherente con la vía conocida de 10 Mbps a 100 Mbps. Ver Tabla 1.

	100Base-TX	**1000Base-X**	**1000Base-T**
Formato de Estructura	802.3 Ethernet	802.3 Ethernet	802.3 Ethernet
Protocolo MAC	802.3 Ethernet	802.3 Ethernet	802.3 Ethernet
Control de Flujo	802.3x	802.3x	802.3x
Velocidad de Símbolo	125Mbaud	125Mbaud	1.25Gbaud
Velocidad de Datos	100Mbps	1000Mbps	1000mbps
Codificación (PCS)	ANSI FDI 4B/5B	ANSI 8B/10B	5 level PAM

Notas:
MAC: Protocolo Media Access Control (Control de Acceso al Medio).
PCS: Physical Coding Sublayer (Subnivel de Codificación Física).
PAM: Pulse Amplitude Modulation (Modulacion por Amplitud de Pulso).

En la actualidad, la ventaja está en las redes que funcionan Fast Ethernet (100Base-TX y 100Base-FX) y tecnologías Gigabit Ethernet. De cara al futuro, se prevé una norma de 10 Gigabit Ethernet; compatibilidad con redes anteriores de 1000 Mbps.

Tabla 1. Compatibilidad 100Base-TX, 1000Base-X y 1000Base-T

1.2.1.3.3 Velocidades Gigabit posibles

Con la llegada de las normas 1000BASE-T, Gigabit Ethernet puede implementarse ahora en toda una red, ya sea sobre cable de fibra óptica o de cobre de categoría 5. Una solución global a 1000 Mbps ofrece varias ventajas.

- *Uso total del ancho de banda:* Se puede conseguir un ancho de banda adicional de hasta 16 Gbps a través de la incorporación del puerto Gigabit, utilizando adaptadores y switches de red. Capacidad de transmisión full-dúplex, sobre fibra o cobre, que permite que los datos se transmitan y se reciban a la vez, lo que duplica realmente el ancho de banda.

- *Calidad y Fiabilidad:* Gigabit Ethernet admite las técnicas de gestión de tráfico existentes que ofrecen calidad de servicio en Ethernet, como prioritización del tráfico IEEE 802.1p y protocolo de reserva de recursos (RSVP). Las pruebas de terceros han demostrado que el índice de errores de bit de 1000BASE-T es inferior a uno en 10.000 millones (lo mismo que para Fast Ethernet y Gigabit sobre fibra). 1000BASE-T es una tecnología muy fiable, que se puede desplegar con total seguridad en redes fundamentales para la empresa.

- *Fácil Migración:* Gigabit Ethernet es totalmente compatible con dispositivos y nodos existentes Ethernet y Fast Ethernet. Gigabit Ethernet utiliza todas las especificaciones definidas por la norma Ethernet original, incluido: técnica de acceso al medio CSMA/CD; estructura Ethernet o formato de trama; control de flujo y objetos de gestión tal como se definen en la norma IEEE 802.3.

- Rentabilidad Económica: Los costos de formación son mínimos porque el personal informático ya está familiarizado con las normas Ethernet. La posibilidad de implementar Gigabit Ethernet en cable de cobre o de fibra óptica ofrece amplias posibilidades de despliegue ya que se utiliza gran parte de la infraestructura existente. De este modo, se reducen al mínimo los gastos en nuevo cableado. Se pueden evitar costosos cambios de tecnología y se reducen al mínimo las paradas de la red.

1.2.1.4 VLANs

Una red LAN fue originalmente definida como una red de hosts localizados dentro de una misma área. Hoy, las LANs son definidas como un solo dominio de broadcast. Esto significa que si un usuario realiza un broadcast en su LAN, el broadcast será recibido por todos los usuarios en la LAN. El broadcast es prevenido utilizando enrutadores entre las LANs. La desventaja de este método es que los enrutadores usualmente toman más tiempo para el proceso de datos de entrada comparado con un switch o bridge. Más importante, la formación de los dominios de broadcast dependen de la conexión física de los dispositivos en la red. Las Redes de Área Local Virtuales (VLANs, Virtual Local Area Networks) fueron desarrolladas como una alternativa de solución para dejar de usar enrutadores para contener el tráfico de broadcast.

1.2.1.4.1 ¿Qué es una VLAN?

En una LAN tradicional, los hosts están conectados uno con el otro por medio de concetrador o un repetidor. Estos dispositivos propagaban cualquier tipo de tráfico generado a través de la red. Sin embargo, si dos hosts intentan enviar información al mismo tiempo, una colisión ocurrirá y toda la transmisión será perdida. Una vez que la colisión ha ocurrido, esto será continuamente propagado a través de la red por los concentradores y los repetidores. La información original, por lo tanto, necesita ser reenviada después de esperar que la colisión haya sido resuelta, de tal modo que, se incurre en un desperdicio significativo de tiempo y de recursos. Para evitar que las colisiones se propaguen a los hosts a través de la red, un switch o un bridge debe ser usado. Estos dispositivos no reenvían colisiones, pero permiten la propagación del broadcast (para cada host en la red) y el multicast (para un grupo de hosts en específico) para pasar a través de la red. Un enrutador puede ser usado para evitar el tráfico por broadcast y multicast para propagarse a través de la red.

Los hosts, concentradores y repetidores juntos forman un segmento de red LAN. Un segmento de red LAN es también conocida como un dominio de colisión puesto que sigue habiendo las colisiones dentro del segmento de red LAN. El área dentro de la cual el broadcast y el multicast son confinados es llamado dominio de broadcast o LAN. En este sentido una LAN puede consistir de uno o más segmentos de red LAN. Definir broadcast y el dominio de colisión en una LAN depende de como los hosts, switches y enrutadores son físicamente conectados juntos. Esto significa que cada uno en una LAN debe ser localizado en la misma área, como se muestra la Figura 16.

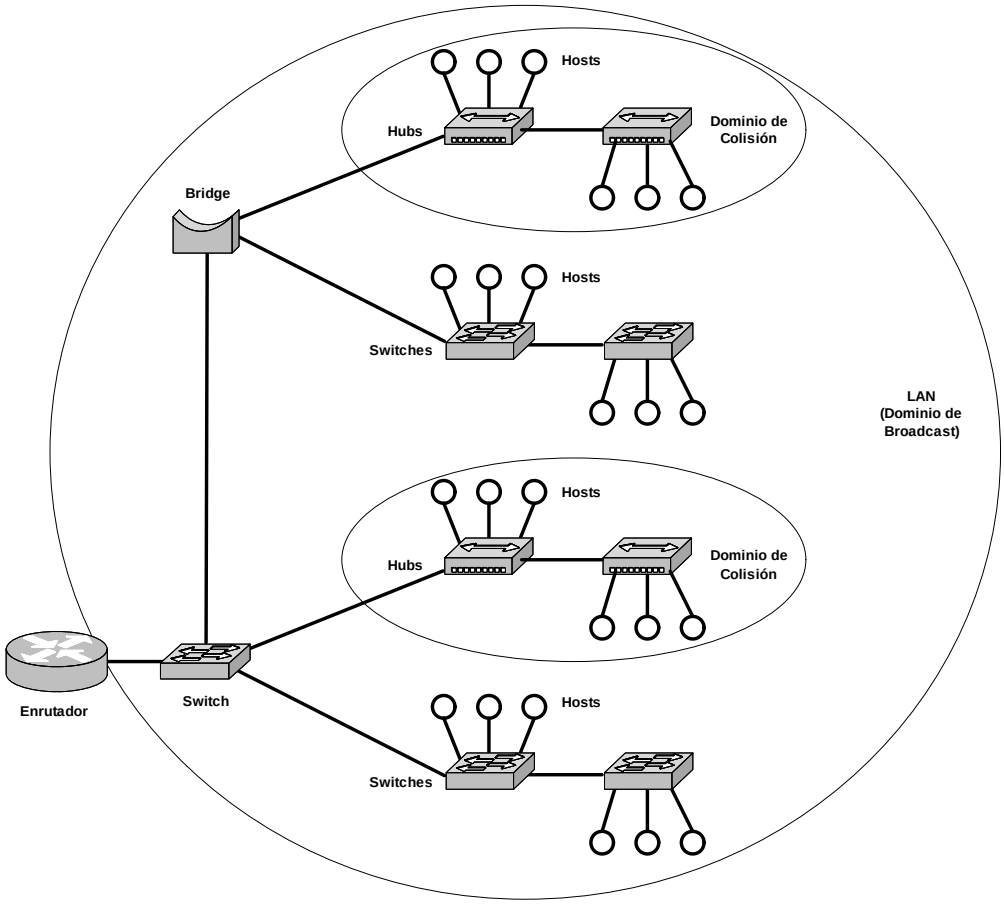


Figura 16. Vista física de una LAN.

Las VLANs permiten administrar una red para segmentar lógicamente una red dentro de diferentes dominios de broadcast (vista lógica, figura 17 y vista física, figura 18). Desde que ésta es una segmentación lógica y no física, los hosts no tienen que ser localizados físicamente juntos. Los usuarios en diferentes pisos de un mismo edificio, o incluso en los edificios diferentes pueden pertenecer ahora al mismo segmento de red LAN.

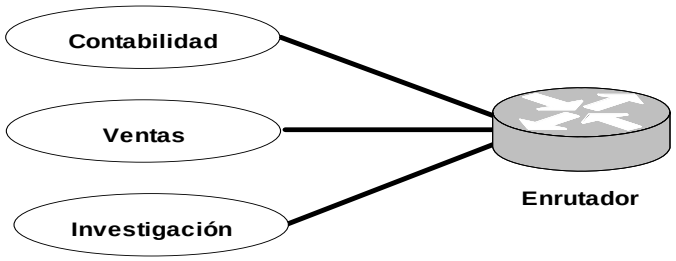


Figura 17. Vista lógica de una VLAN.

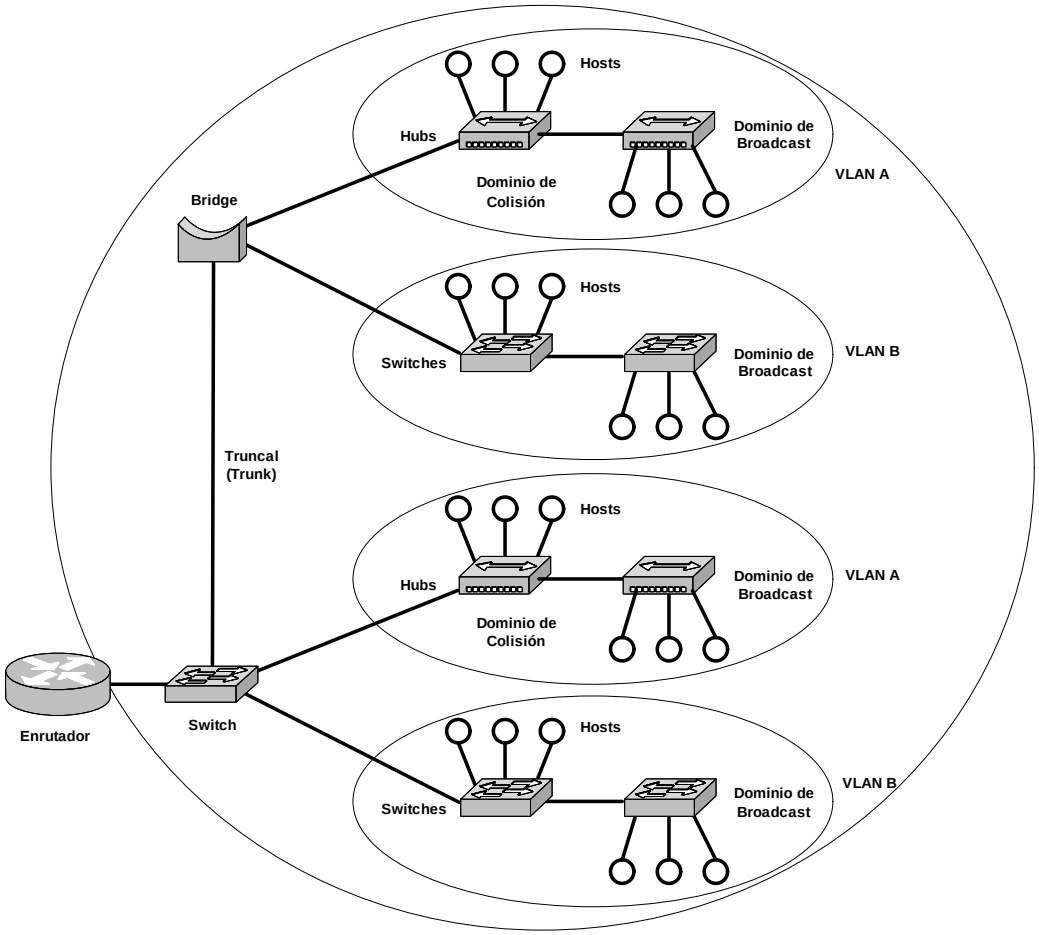


Figura 18. Vista física de una VLAN.

Las VLANs también permiten dominios de broadcast para ser definidos sin usar enrutadores. El software de Bridging es usado en cambio para definir que hosts son para ser incluidos en el dominio de broadcast. Los enrutadores podrían ser usados para comunicar VLANs.

1.2.1.4.2 ¿Por qué implementar VLANs?

Las VLANs ofrecen un número de ventajas sobre las tradicionales LANs. Estas son:

1) **Desempeño.** En las redes donde el tráfico consisten de un alto porcentaje de broadcast y multicast, las VLANs pueden reducir la necesidad para enviar tanto tráfico para destinatarios innecesarios. Por ejemplo, un dominio de broadcast consiste en 10 usuarios, si el tráfico de broadcast es intentado solo para 5 usuarios, entonces poniendo a esos 5 usuarios en una VLAN diferente, puede reducir el tráfico.Comparando los switches, los enrutadotes requieren más procesamiento para el tráfico de entrada. Como el volumen de tráfico que pasa a través de los enrutadores aumenta, entonces hace la latencia en los enrutadores,

la cual es el resultado de reducir el desempeño. El uso de VLANs reduce el número de enrutadores necesarios, desde la creación de dominios de broadcast de VLANs usando switches en lugar de enrutadores.

2) **Formación de Grupos de Trabajo Virtuales.** Hoy día, es común encontrar a equipos funcionales del desarrollo de productos con los miembros de diferentes departamentos como mercadotecnia, ventas, contabilidad e investigación. Esos grupos son usualmente formados por un periodo corto de tiempo. Durante este periodo, la comunicación entre miembros de los grupos de trabajo será alta. Para contener el broadcast y multicast dentro del grupo de trabajo, una VLAN puede ser configurada para ellos. Con las VLANs es fácil para ubicar miembros de un grupo de trabajo juntos. Sin las VLANs, la única manera para que esto pueda ser posible es mover físicamente a todos los miembros del grupo de trabajo juntos.Sin embargo, los grupos de trabajo virtuales no vienen sin los problemas. Considerar la situación donde un usuario del grupo de trabajo es uno de cuatro pisos de un edificio, y los otros miembros del grupo de trabajo están en el segundo piso. Los recursos como impresoras podrían ser ubicados en el segundo piso, el cual podría ser inconveniente para el usuario solitario del piso. Otro problema con la configuración de grupos de trabajo virtuales es la implementación de la granja de servidores centralizada, los cuales son esencialmente colecciones de servidores y mayores recursos para operar la red en una ubicación centralizada. La granja de servidores centralizada puede provocar problemas cuando se configura un grupo de trabajo virtual, si los servidores no pueden ser ubicados en más que una VLAN. En este caso, el servidor podría ser ubicado en una sola VLAN y las VLANs restantes intentarán acceder el servidor a través de un enrutador, esto puede reducir el desempeño.

3) **Administración Simplificada.** El 70% del costo de las redes son como el resultado de agregar, mover o cambiar usuarios dentro de la red. Cada que un usuario es movido dentro de la LAN, re-cablear, nuevo direccionamiento, y re-configuración de switches y enrutadores se convierten necesarias. Algunas de esas tareas pueden ser simplificadas con el uso de VLANs. Si un usuario es movido dentro de una VLAN la configuración del enrutador no es necesaria. Además, depende del tipo de VLAN, otro trabajo que puede ser reducido o eliminado. Sin embargo, el poder de las VLANs solo se siente cuando se crean las herramientas de administración las cuales pueden permitir a los administradores de red asociar o desasociar usuarios dentro de diferentes VLANs.

4) **Reducir Costos.** Las VLANs pueden ser usadas para crear dominios de broadcast, las cuales eliminan la necesidad de enrutadores, que generalmente son más caros que los switches.

5) Seguridad. Es normal que los datos confidenciales sean transmitidos dentro de la red. En estos casos, asignar una VLAN a los usuarios que necesitan tener esos datos confidenciales puede reducir las posibilidades de que un usuario no válido tenga acceso a ellos. Las VLANs pueden también, ser usadas para controlar dominios de broadcast, configurar Firewalls, restringir el acceso e informar al administrador de red del acceso de intrusos.

1.2.1.4.3 ¿Cómo trabajan las VLANs?

Cuando un switch recibe una trama de un host, este etiqueta la trama con un identificador de VLAN indicando de que VLAN viene. Este proceso es llamado explícitamente como tagging (etiquetado). Esto permite determinar a que VLAN pertenece la trama, usando etiquetado implícito. En el etiquetado implícito, las tramas no son etiquetadas, pero las tramas de cierta VLAN son identificados basándose en otra información, como el puerto donde la trama ha llegado. El etiquetado puede ser basado en el puerto del cual proviene la trama, del campo de la dirección MAC origen, la dirección de red origen, o algún otro campo o una combinación de campos. Las VLANs son clasificadas basadas en el método usado. Para ser capaz de etiquetar las tramas usando cualquiera de esos métodos el switch tendría que guardar una base de datos de actualizada al día que contenga un mapa entre las VLANs y cualquier campo que sea utilizado para etiquetar. Por ejemplo, si se etiquetara por puerto, la base de datos debe indicar cuáles puertos pertenece pertenecen a que VLAN. Esta base de datos es llamada base de datos de filtrado. Los switches tendrían que poder mantener esta base de datos y también para asegurarse que todos los switches en la LAN tienen la misma información en cada una de sus bases de datos. Los switches definen donde se van las tramas basándose en el funcionamiento normal de una LAN. Una vez que el switch determina hacia donde van las tramas, este ahora necesita determinar si el identificador de VLAN debe ser agregado a la trama y enviarlo. Si la trama va a un dispositivo que conoce acerca de la implementación de VLAN (VLAN-aware), el identificador de VLAN es agregado a la trama. Si va a un dispositivo que no tiene conocimiento de las VLANs (VLAN-unaware), los switches mandan la trama sin etiquetado.

Para entender como trabajan las VLANs, es necesario conocer los tipos de VLANs, los tipos de conexiones entre dispositivos en una LAN, la base de datos de filtrado la cual es usada para enviar el tráfico a la VLAN correcta, y etiquetado, un proceso usado para identificar las tramas que se originan en las VLANs.

1.2.1.4.3.1 Tipos de VLANs

Los miembros de una VLAN pueden ser clasificados por puerto, la dirección MAC y el tipo de protocolo.

1) Capa 1 VLAN: miembros por puerto. Los miembros en una VLAN puede ser definido basado en los puertos que pertenecen a la VLAN. Por ejemplo, en un switch con cuatro puertos, los puertos 1, 2 y 4 pertenecen a la VLAN 1 y el puerto 3 a la VLAN 2. Ver tabla 2.

Puerto	VLAN
1	1
2	1
3	2
4	1

Tabla 2. Asignación de puertos a diferentes VLANs.

La principal desventaja de este método es que no permite la movilidad del usuario. Si un usuario es movido a una localidad diferente fuera del switch asignado, el administrador de red debe de configurar nuevamente la VLAN, y por supuesto, debe existir comunicación basada en algún tipo de conexión, que se tocará más adelante, entre el nuevo lugar y la VLAN anterior.

2) Capa 2 VLAN: miembros por dirección MAC. Aquí, los miembros de una VLAN están basaos en la dirección MAC de cada host. El switch rastrea la dirección MAC para saber a que VLAN pertenece (tabla 3). Desde que la dirección MAC forma parte de la tarjeta de red (NIC, Network Interface Card) de los hosts, cuando un host es movido, no es necesario configurar para permitir al host que permanezca a la misma VLAN. Esto es lo contrario de las VLANs de capa 1 donde los miembros deben ser configurados nuevamente.

Dirección MAC	VLAN
00-08-02-D6-FE-C9	1
00-02-2D-1E-3C-86	2
00-50-04-05-E3-FC	2
00-E0-29-50-C5-CD	1

Tabla 3. Asignación de direcciones MAC a diferentes VLANs.

El principal problema con este método es que los miembros de la VLAN deben ser asignados en un principio, es decir, se debe conocer la dirección MAC del host antes de configurarlo a la VLAN. En las redes con miles de usuarios, no es una tarea fácil. Además, en ambientes donde los hosts portátiles son indispensables, la dirección MAC es asociada con el docking station (base de portátil) y no con el host portátil. Consecuentemente, cuando un portátil es movido a una docking station diferente, este miembro de la VLAN debe de ser configurado nuevamente.

3) Capa 2 VLAN: miembros por tipo de protocolo. Los miembros de una VLAN de VLANs de capa 2 pueden ser basados en el campo de tipo de protocolo encontrado en el encabezado de capa 2.

Protocolo	VLAN
IP	1
IPX	2

Tabla 4. Asignación de protocolos a diferentes VLANs.

4) Capa 3 VLAN: miembros por dirección de subred IP. Los miembros están basados en el encabezado de capa 3. Las subredes pueden ser usadas para clasificar los miembros de una VLAN. Tabla 4.

Subred IP	VLAN
192.168.1.0	1
172.16.7.0	2

Tabla 5. Asignación de subredes IP a diferentes VLANs.

Aunque los miembros de una VLAN estén basados en información capa 3, esto no tiene que ver con la enrutamiento de redes y no debe de ser confundido con las funciones de enrutamiento. En este método, el direccionamiento IP es usado solamente como mapeo para determinar los miembros de las VLANs. Ningún otro proceso con direcciones IP es realizado. En las VLANs de capa 3, los usuarios pueden mover sus hosts sin configurar nuevamente sus direcciones de red. El único problema es que generalmente toma mucho más tiempo reenviar los paquetes usando la información de capa 3 en lugar de la dirección MAC.

5) VLANs de capa superior. También es posible definir miembros de VLANs basados en aplicaciones o servicios, o cualquier combinación de ellos. Por ejemplo, aplicaciones como el FTP (File Transferir Protocol) pueden ser ejecutadas en una VLAN y el TELNET en otra.

La norma 802.1Q, define solamente las VLANs de capa 1 y 2. Y las VLANs basadas en protocolos y capas superiores son implementaciones propietarias de cada fabricante de Switches.

1.2.1.4.3.2 Tipos de conexiones

Los dispositivos en una VLAN pueden ser conectados de tres maneras basadas en sí los dispositivos conectados son VLAN-aware o VLAN-unaware. La llamada que un dispositivo VLAN-aware es una la cual entienden los miembros de las VLANs (por ejemplo, que usuarios pertenecen a una VLAN) y formatos de las VLANs.

1) Enlace troncal. Todos los dispositivos conectados a un enlace troncal, incluyendo hosts, deben ser VLAN-aware. Todas las tramas en un enlace troncal deben tener un encabezado especial agregado. Esas tramas especiales son llamadas tramas etiquetadas. Ver figura 19.

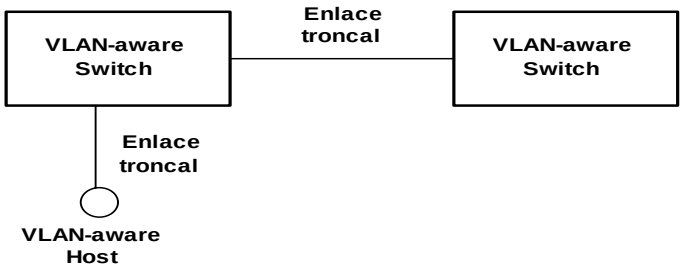


Figura 19. Enlace troncal entre dos Switches VLAN-aware.

2) Enlace de acceso. Un enlace de acceso conecta dispositivos VLAN-unaware para el puerto de un Switch VLAN-aware. Todas las tramas en enlaces de acceso deben ser etiquetadas implícitamente (sin etiquetar), ver figura 20. Los dispositivos VLAN-unaware pueden ser un segmento LAN con hosts VLAN-unaware o esto puede ser un número de segmentos LAN que contienen dispositivos VLAN-unaware.

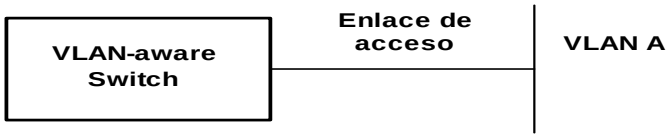


Figura 20. Enlace de acceso entre un Switch VLAN-aware y un dispositivo VLAN-unaware.

3) Enlace híbrido. Esta es una combinación de los enlaces anteriores. Este es un enlace donde ambos dispositivos VLAN-aware y VLAN-unaware están adjuntos, ver figura 21. Un enlace híbrido puede tener ambas tramas, etiquetadas y sin etiquetar, pero todas la tramas para una VLAN específica deben ser etiquetadas o no estiquetadas.

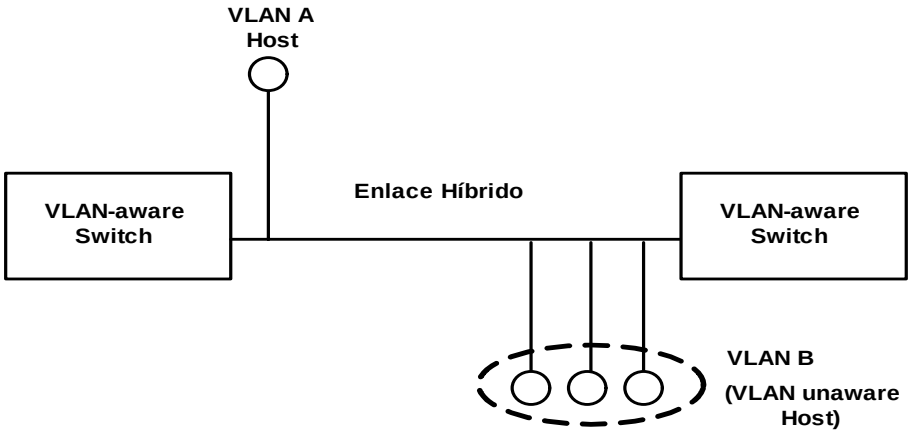


Figura 21. Enlace híbrido contiene ambos dispositivos, VLAN-aware y VLAN-unaware.

1.2.1.4.3.3 IEEE 802.1Q

La especificación IEEE 802.1Q establece un método estándar para etiquetar (VLAN tagging) las tramas Ethernet con la información de los miembros de las VLANs. El protocolo 802.1Q fue desarrollado por el problema de crecimiento de direccionamiento que tenían los administradores de red: como romper una red larga switcheada en pequeños segmentos lógicos para que el tráfico de broadcast y multicast, no agrave mucho la disponibilidad del ancho de banda, así como proporcionar un mayor nivel de seguridad entre los segmentos internos de la red, ya que, el único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible “escuchar" la información si no nos es permitida, porque ese tráfico de información no pasa físicamente por ese segmento.

1.2.1.4.3.4 Prioridad y VLANs para Ethernet – Un nuevo formato de trama

La norma de etiquetado de VLAN 802.1Q, fue introducida con la norma de etiquetado de prioridad 802.1p. Cada norma utiliza pocos bits del encabezado (header) de la trama Ethernet para mantener la etiqueta.

El etiquetado de tramas con información 802.1p y 802.1Q es hecha en la capa de enlace, no en la de red. Por lo tanto, implantar cualquiera de los dos, prioridad o etiquetado VLAN requiere un cambio en el formato de trama Ethernet de la norma 802.3. La norma 802.3ac define el nuevo formato de trama que implanta campos de información del 802.1p y 802.1Q VLAN. La figura 22, muestra la trama convencional de Ethernet.

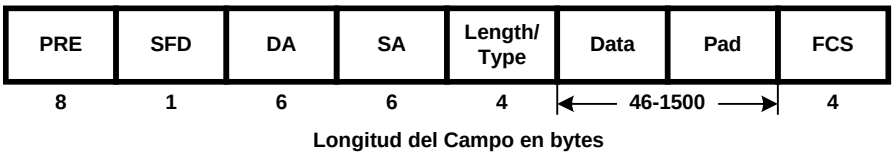


Figura 22. Formato de trama 802.3 antes de 802.1p y 802.1Q.

En la figura 23, se muestra el nuevo formato de trama 802.3ac. Los campos sombreados representan la suma de 802.1p y el etiquetado 802.1Q.

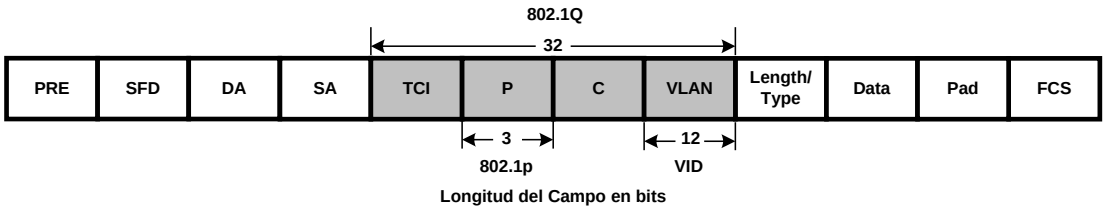


Figura 23. Nuevo formato de trama 802.3, incluyendo 802.1p y 802.1Q.

Definición de cada uno de los campos de la figura 23:

Etiqueta	Nombre del Campo	Tamaño	Descripción
PRE	Preamble	7 bytes	Usado para sincronizar el tráfico entre nodos
SFD	Start Trama Delimiter	1 bytes	Marca el comienzo del encabezado
DA	Destination Address	6 bytes	Dirección MAC destino
SA	Source Address	6 bytes	Dirección MAC origin
TCI	Tag Control Info	2 bytes	Cuando se ajusta en “8100”, indica el uso de las tramas 802.1p y etiquetado 802.1Q
P	Priority	3 bits	Indica el nivel de prioridad (0-7) 802.1p
C	Canonical Indicator	1 bit	Indica si la dirección MAC está en formato canónico – Ethernet usa “0”
VLAN	VLAN Identifier (VID)	12 bits	Indica a cual VLAN pertenece esta trama pertenece (0-4095)
Length/Type	Length/Type Field	2 bytes	Tipo Ethernet II o 802.3 / Longitud de información
Data y Pad	Payload	≤ 1500 bytes	Datos de usuario o información para protocolos de capas superiores
FCS	Trama Check Sequence	4 bytes	Comparación del contenido de tramas, también conocido como CRC

Tabla 6. Descripción de campos de 802.3.

Los valores insertados en los nuevos campos cuentan por 4 bytes adicionales de datos en la trama Ethernet. El nuevo campo TCI siempre tiene el valor de 8100 en hexadecimal. El campo de prioridad especifica uno de ocho posibles valores disponibles de prioridades 802.1p (0-7). El campo del identificador canónico significa el orden de los bits en el campo VLAN ID (Ethernet tiene normalmente este bit ajustado en 0). Finalmente, el identificador de VLAN (VID) asigna la trama de uno a 4093 posibles VLANs (2 – 4094, los VIDs 0, 1, y 4095 son reservados).

1.2.1.4.3.5 Consideraciones de desarrollo para el nuevo formato de trama 802.1p/Q

Un problema que se da al implantar 802.1Q en una red existente, es que la adición de campos de etiquetado incrementa al máximo el tamaño de la trama (sin contar los campos de Preámbulo y Stara Trama Delimiter) a 1522 bytes, en cambio el máximo tamaño de la trama Ethernet es de 1518 bytes. Esto puede causar problemas en la migración. Mucho equipo de interconexión manufacturado antes de 1998 categoriza todas las tramas superiores que 1518 bytes, como tramas de sobre tamaño (giagiant), éstos asumen que son tramas corruptas y las tiran.

Estos problemas pueden superarse, al conectar switches que soporten 802.1p y 802.1Q (802.3ac) por los que no lo soporten.

1.2.1.5 WLAN:

Las comunicaciones inalámbricas, pueden clasificarse de distintas formas dependiendo del criterio al que se atienda. En este caso, se clasificarán los sistemas de comunicaciones inalámbricas de acuerdo con su alcance. Se llama alcance a la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica.

WPAN	WLAN	WMAN	Celular
<10 metros	Edificio Campus	Ciudad	Región Global
Bluetooth 802.15 IrDA	Wi-Fi HomeRF HiperLAN	LMDS MMDS 802.16	2G 2.5G 3G

Tabla 7. Tipo de redes inalámbricas.

La IEEE, en junio de 1997, aprobó la primera norma 802.11 que define el nivel físico y la subcapa MACpara las transmisiones inalámbricas en una red de área local, mostrado en la Figura 24.

MODELO OSI	IEEE 802.11	TÉCNICAS DE DIFUSIÓN DE 802.11					
Capa de Enlace	LLC MAC						
Capa Física	PLCP PMD	DSSS 802.11	FHSS 802.11	Infrarrojos 802.11	DSSS-HR 802.11b	OFDM 802.11a	OFDM 802.11g

Figura 24. Arquitectura de la norma IEEE 802.11.

La primera norma 802.11 utilizaba infrarrojos como medio de transmisión. Esta operaba en la banda de 850 a 950 nm, utilizaba la modulación PPM de 4 ó 16 niveles. Esta norma nunca tuvo una buena aceptación en el mercado debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a las interferencias producidas por agentes naturales como la lluvia o niebla.

Posteriormente, salieron otras dos normas 802.11 basadas en el uso de microondas en la banda 2.4 GHz, banda del ISM (Industrial, Scientific and Medicine), empleando tecnología de espectro disperso o extendido. Ambas se diferenciaban por el método de transmisión utilizado. Una utilizaba FHSS (Frequency Hopping Spread Spectrum, Difusión por Salto de Frecuencia) y la otra, el sistema DSSS (Direct Sequence Spread Spectrum, Difusión por Secuencia Directa). DSSS utilizaba modulación DBPSK (Differential Binary Phase Shift Keying, Modulación Diferencial Binaria por Salto de Fase) y DQPSK (Differential Quadrature Phase Shift Keying, Modulación Diferencial de Cuadratura por Salto de Fase) proporcionando 1 Mbps y 2 Mbps, respectivamente. Mientras que, FHSS usaba 2GFSK (2-Level Gaussian Frequency Shift Keying, Modulación Gausiana por Salto de Frecuencia de 2 Niveles) y 4GFSK (4-Level Gaussian Frequency Shift Keying, Modulación Gausiana por Salto de Frecuencia de 4 Niveles), proporcionando un bit rate de 1 Mbps ampliable a 2 Mbps bajo condiciones de operación óptimas.

En 1999 el grupo de trabajo 802.11 aprobó dos extensiones a la norma 802.11:

- *IEEE 802.11b.* Esta norma opera en los 2.4 GHz. Subía la velocidad de transmisión a los 11 Mbps. Por este motivo se la conoció también como 802.11 HR (High Rate, Alta Velocidad).

- *IEEE 802.11a.* Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de los 2.4 GHz, sino la de los 5 GHz y que utiliza una técnica de transmisión conocida como OFDM (Orthogonal Frequency Division Multiplexing, Multiplexación Ortogonal por División de Frecuencia). La gran ventaja es que se consiguen velocidades de 54 Mbps; llegándose a alcanzar los 72 Mbps y 100 Mbps con versiones propietarias de esta tecnología. El mayor inconveniente es que la tecnología de semiconductores para 5 GHz no está suficientemente desarrollada todavía.

Pero eso no fue todo, en el año 2001, surgió la norma IEEE 802.11g con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2.4 GHz. Esta norma permite transmitir datos a 54 Mbps, utilizando OFDM. La característica que lo hace especialmente interesante es su compatibilidad con 802.11b, y que tienen mayor alcance y menor consumo de potencia que los equipos que utilizan 802.11a. En cualquier caso, existen versiones propietarias de esta tecnología que llega a los 100 Mbps.

Norma	Grupos de Trabajo
802.11 (1997)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas (infrarrojo y microondas 2.4 GHz)
802.11a (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas (microondas 5 GHz)
802.11.b (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas de rango de velocidades de 5.5 a 11 Mbps (microondas 2.4 GHz)
802.11c	Gateway MAC entre redes
802.11e	QoS, Quality of Service. Calidad de servicio para aplicaciones avanzadas (voz, video, etc.)
802.11f (2000)	Interoperatividad entre puntos de acceso de distintos fabricantes (Interaccess Point Protocol, IAPP)
802.11g (2001)	Especificaciones para redes inalámbricas de alta velocidad (54 Mbps) en la banda de 2.4 GHz
802.11h	Mejoras para la selección dinámica de canal y control de potencia de transmisión
802.11i	Mejoras para seguridad y autenticación
5GSG	Globalización de los 5 GHz, grupo de estudio junto con ETSI/BRAN (European Telecommunications Standard Institute/Broadband Radio Area Network, Instituto Europeo de Normalización en Telecomunicaciones/Redes Vía Radio de Banda Ancha) y MMAC (Mobile Multimedia Access Communication, Comunicaciones Multimedia de Acceso Móvil) de Japón para promover la interoperatividad entre 802.11a, ETSI HiperLAN/2 y MMAC

Tabla 8. Grupos de trabajo y de estudio relacionados con IEEE 802.11.

En el interés de disponer de normas inalámbricas lo antes posible, al desarrollar sus normas, la IEEE no considero determinadas características (como la calidad de servicio, seguridad, utilización del espectro, etc.) que seguramente hubieran producido una norma

más robusta. Para resolver este problema, el IEEE ha creado posteriormente unos grupos de trabajo, mostrados en la tabla 3, para desarrollar normas que resuelvan estos problemas y que puedan ser añadidos fácilmente al protocolo principal. Algunos grupos son los siguientes:

- *IEEE 802.11e* (Calidad de servicio). Este grupo trabaja en los aspectos relacionados con la calidad de servicio. En el mundo de las redes de datos, calidad de servicio significa poder dar más prioridad a unos paquetes de datos que a otros, dependiendo de la naturaleza de la información (voz, video, imágenes, etc.).

- *IEEE 802.11h* (Gestión del espectro). Este grupo de trabajo pretende conseguir una mejora de la norma IEEE 802.11a en cuanto a la gestión del espectro radioeléctrico. Este punto es una de las desventajas que tiene IEEE 802.11a frente a su competidor europeo HiperLAN/2, que también opera en la banda de 5 GHz.

- *IEEE 802.11i* (Seguridad). El sistema de seguridad que utiliza 802.11 está basado en el sistema WEP (Wired Equivalency Protocol, Protocolo de Equivalencia con Red Cableada). Este sistema ha sido fuertemente criticado debido a su debilidad. Este grupo de trabajo pretende sacar un nuevo sistema mucho más seguro que sustituya a WEP. El sistema sobre el que está trabajando se conoce como TKIP (Temporal Key Integrity Protocol, Protocolo de Integridad de Clave Temporal).

El problema principal que pretende resolver la normalización es la compatibilidad. No obstante, existen distintas normas que definen distintos tipos de redes inalámbricas. Esta variedad produce confusión en el mercado, descoordinación en los fabricantes, y por supuesto, problemas para diseñar una red debido a que no deja abierta la posibilidad de utilizar cualquier marca. Para resolver este problema los principales fabricantes (3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies) crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compability Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). El objetivo de esta asociación fue crear una marca que permita fomentar fácilmente la tecnología inalámbrica y asegurarse de la compatibilidad de equipos.

De esta manera, desde abril de 2000, WECA certifica la interoperatividad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi (Wireless Fidelity, Fidelidad Inalámbrica). Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos. En el año 2002 eran casi 150 los miembros de la asociación WECA.

Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps y ya existen normas que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por esta razón, WECA también certifica los equipos IEEE 802.11a de la banda de 5 GHz.

1.2.1.5.1 Las capas de IEEE 802

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del modelo OSI: la capa física y la capa de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas:

- PHY (Physical Layer, Capa Física) es la capa que se ocupa de definir los métodos por los que se difunde la señal.

- MAC (Medium Access Control, Control de Acceso al Medio) es la capa que se ocupa del control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La subcapa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.

- LLC (Logical Link Control, Control de Enlace Lógico) es la subcapa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

1.2.1.5.2 La Capa Física

La capa física se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas lo que se conoce como PLCP (Physical Layer Convergence Procedure, Procedimiento de Convergencia de la Capa Física) y PDM (Physical Medium Dependent, Dependiente del Medio Físico). PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de microondas, mientras que PDM es la que se encarga de la difusión de la señal.

Por cierto, aunque las especificaciones originales de IEEE 802.11 contemplan la opción de utilizar infrarrojos como medio de transmisión, no obstante, nunca ha llegado a desarrollarse este sistema debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a las interferencias producidas por agentes naturales como la lluvia o la niebla.

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricos es el sistema conocido como espectro extendido o disperso. Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistentes a los efectos de eco o multitrayectorias y que puede coexistir con otros sistemas de radiofrecuencia sin verse afectado y sin influir en su actividad. Estas ventajas hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no necesita licencia.

Existen distintas técnicas de espectro expandido, entre las que se encuentra la tecnología CDMA utilizada en tercera generación de telefonía móvil. No obstante IEEE 802.11 contempla solo dos técnicas distintas de espectro expandido:

- *FHSS* (Frequency Hopping Spread Spectrum, Espectro Expandido por Salto de Frecuencia), con la que consiguen velocidades de transmisión de 1 Mbps. Esta técnica consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos (*spreading code o hopping code*) conocido tanto por el emisor como por el receptor. El tiempo máximo que debe permanecer en cada frecuencia esta regulado en 400 ms.

- *DSSS* (Direct Sequence Spread Spectrum, Espectro Expandido por Secuencia Directa), con la que se consiguen velocidades de transmisión de 2 Mbps. En versiones posteriores de este sistema se han conseguido velocidades superiores. La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como chip o código de chips (*chipping code*). Estos códigos de chips permiten a los receptores eliminar por filtrado de señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

Dependiendo de la velocidad a la que se fueran a transmitir los datos, la norma IEEE 802.11 utilizaba una técnica u otra.

En 1999 el IEEE sacó una nueva versión de DSSS que permite transmitir datos a 11 Mbps. Esta nueva DSSS está recogida en la norma IEEE 802.11b. Por esta razón, al 802.11b se le conoce como 802.11 DSSS ó 802.11 HR.

A pesar de esto, en la práctica, la velocidad de 11 Mbps no es totalmente real debido a distintas razones:

- Las interferencias y ruidos hacen que la velocidad real baje.
- El propio protocolo consigue menos rendimiento que en sistemas cableados.
- Las conexiones a los puntos de acceso son un cuello de botella.
- El ancho de banda es compartido.

Por otro lado, la mayoría de las tarjetas inalámbricas de los hosts son half-duplex (semiduplex), solo contienen un equipamiento de radio, por lo que pueden transmitir o recibir, pero no ambas cosas simultáneamente.

Además de las técnicas de difusión comentadas anteriormente, con la nueva versión IEEE 802.11a salió una nueva técnica conocida como OFDM, es una técnica de gestión de frecuencias. Esta técnica divide el ancho de banda en subcanales más pequeños que operan en paralelo. De esta manera se consiguen velocidades de transmisión de hasta 54 Mbps y 100 Mbps con soluciones propietarias.

Velocidad de transmisión	Técnica de Modulación	Técnica de Difusión
1 Mbps	DBPSK	DSSS
2 Mbps	DQPSK	DSSS
5.5 Mbps	CCK	DSSS
11 Mbps	CCK	DSSS

Tabla 9. Técnicas de modulación utilizadas por IEEE 802.11b.

Velocidad de transmisión	Técnica de Modulación	Técnica de Difusión
6 Mbps	BPSK	OFDM
9 Mbps	BPSK	OFDM
12 Mbps	QPSK	OFDM
18 Mbps	QPSK	OFDM
24 Mbps	QAM-16 (BPSK)	OFDM
36 Mbps	QAM-16 (BPSK)	OFDM
48 Mbps	QAM-64 (QPSK)	OFDM
54 Mbps	QAM-64 (QPSK)	OFDM

Tabla 10. Técnicas de modulación utilizadas por IEEE 802.11a.

Velocidad de transmisión	Técnica de Modulación	Técnica de Difusión
1 Mbps	DBPSK	DSSS
2 Mbps	DQPSK	DSSS
5.5 Mbps	CCK	DSSS
11 Mbps	CCK	DSSS
6 Mbps	BPSK	OFDM
9 Mbps	BPSK	OFDM
12 Mbps	QPSK	OFDM
18 Mbps	QPSK	OFDM
24 Mbps	QAM-16 (BPSK)	OFDM
36 Mbps	QAM-16 (BPSK)	OFDM
48 Mbps	QAM-64 (QPSK)	OFDM
54 Mbps	QAM-64 (QPSK)	OFDM

Tabla 11. Técnicas de modulación utilizadas por IEEE 802.11g.

1.2.1.5.2.1 Modulación de la señal.

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la señal. La modulación consiste en modificar una señal pura de radio para incorporarle la señal a transmitir. La señal base a modular recibe el nombre de portadora. Lo que se le cambia a la portadora para modularla es su amplitud, frecuencia, fase o una combinación de éstas. Mientras mayor es la velocidad de transmisión, más complejo es el sistema de modulación. Las técnicas de modulación utilizadas en IEEE 802.11 son: BPSK (Binary Phase-Shift Keying, Modulación Binaria por Salto de Fase), QPSK (Quadrature Phase-Shift Keying, Modulación por Salto de Fase en Cuadratura), GFSK (Gaussian Frequency-Shift Keying, Modulación Gausiana por Salto de Frecuencia), CCK (Complementary Code Keying, Modulación de Código Complementario)

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y demodular la información. Los sistemas de FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia y en el segundo, solo el tiempo.

1.2.1.5.3 La Subcapa MAC

La subcapa MAC define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones de la norma 802.11 utilizan distintos sistemas para difundir su señal (la capa física es distinta), la subcapa MAC es la misma para todas ellas.

Es interesante también el hecho de que la subcapa MAC sea muy similar a la utilizada por la tecnología Ethernet. Ambas utilizan la técnica de acceso al medio conocida como CSMA. No obstante la versión cableada (Ethernet) utiliza la tecnología CD, mientras que la versión inalámbrica utiliza la tecnología CA (Collision Avoidance, Evitación de Colisión). Una colisión se produce cuando dos hosts intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando el medio es un cable, un host puede transmitir y recibir al mismo tiempo, por lo que puede detectar las colisiones. Por el contrario, en el medio radioeléctrico un host no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca a la recepción), por lo que, al no poder detectar las posibles colisiones, no hay más remedio que disponer de una técnica que las evite.

1.2.1.5.3.1 Evitar las colisiones

Entre la subcapa MAC y la capa física se intercambian tres tipos de paquetes de datos: de control, de gestión y de información.

La subcapa MAC tiene dos funciones distintas para coordinar la transferencia de datos:

- *PCF* (Point Coordination Function, Función de Coordinación de Punto) facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial evitando las demoras. El coordinador del punto, PC (Point Coordinator) reside en el Punto de Acceso. El PC emite una señal guía con la duración del periodo de tiempo que necesita disponer del medio. Los hosts que reciben esta señal no emiten durante ese tiempo. El PCF usa un mecanismo de sensado de portadora virtual ayudado por un mecanismo de prioridad de acceso.

- *DCF* (Distributed Coordination Function, Función de Coordinación Distribuida) facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etc.) entre todos los hosts de la red. Para ello, DCF define los mecanismos que aseguran la entrega de los datos a los hosts. A través de DCF se transmiten los datos que no son sensible a retardos. Esta función también es conocida como CSMA/CA, en conjunto con un sistema de reconocimiento (ACK).

Las dos funciones PCF y DCF coexisten en una manera que permite a ambas funciones operar simultáneamente con la misma BSS (Basic Service Set, Conjunto de Servicios Básicos).

La función DCF se encuentra con un problema y es que una de las diferencias de los medios cableados frente a los inalámbricos es que en éstos últimos es mucho más complicado detectar las colisiones. Dos hosts que no se ven entre sí pueden iniciar una comunicación simultáneamente sin percatarse de la colisión. DCF dispone de una función para impedir la colisión que evita este problema.

Los mecanismos CSMA/CA de detección de colisión consisten en comprobar si el medio está en uso antes de empezar a transmitir. Si el medio está en uso, se espera un tiempo antes de volver a hacer la comprobación. El tiempo que espera cada host tiene una duración aleatoria (generada por cada host entre un tiempo mínimo y un máximo) para evitar que haya colisiones sucesivas indefinidas. El host utiliza un algoritmo de Backoff, el cual determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time).

La función DCF contempla un mecanismo físico y otro lógico de detección de colisión. Al mecanismo físico se le conoce como CCA (Clear Channel Assessment, Valoración de la Disponibilidad del Canal). Por ejemplo, cuando se habla de un medio radioeléctrico, este mecanismo puede consistir en comprobar si en el medio existe cualquier señal DSSS o cualquier otra señal con un nivel de energía superior a un umbral.

El mecanismo físico de detección de colisión es muy eficiente, pero no es eficaz cuando dos hosts de una misma red que no se ven entre ellas emiten al mismo tiempo. Esto se conoce con el nombre de problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico de detección de colisión. Este sistema consiste en intercambiar la información del uso del medio a través de tramas de control. A estas tramas de control se las conoce como RTS (Request to Send, Solicitud para Enviar) y CTS (Clear to Send, Listo para Enviar). Como esta información de control añade más datos de control a la transmisión en detrimento de los datos de información (baja el rendimiento del protocolo), en aquellos casos en los que se disponga de un medio físico con poca probabilidad de colisiones se puede deshabilitar el mecanismo de detección de colisión, o habilitarlo exclusivamente para aquellos paquetes de datos que tengan un tamaño superior a uno determinado.

Cuando un host de una red va a transmitir información, primero envía una trama RTS al punto de acceso donde facilita información del destinatario de la transmisión, el remitente y el tiempo que ocupará dicha transmisión. El punto de acceso responde con una trama CTS que reciben todas los hosts que están en el área de cobertura del punto de acceso. En esta trama CTS se incluye el tiempo de ocupación del medio; por tanto, los hosts saben el tiempo que estará ocupado el medio y no intentarán hacer ninguna transmisión hasta que dicho tiempo haya transcurrido. A los tiempos contenidos en estas tramas se les conoce como NAV (Network Allocation Vector, Vector de Asignación de Red).

Por cierto, cuando el destinatario ha recibido toda la información y revisado el CRC, emite una trama ACK para indicarle al emisor que todo está bien. Si el emisor no recibe la trama ACK que espera, aguardará un tiempo antes de dar la transmisión por errónea y volver a hacer el envío.

Además, existen algunos tiempos asociados a estas tramas.

- *SIFS:* Short Intertrama Space. Se usa para separar transmisiones de una misma conexión (una trama ACK, una trama CTS, etc). Sólo hay un host autorizado para transmitir después de este tiempo. El valor de este tiempo se calcula considerando que el host transmisor pueda cambiar a modo recepción y decodificar la trama devuelta. SIFS = 28 µs.

- *PIFS:* PCF Intertrama Space. Usado por hosts operando bajo la función PCF para ganar prioridad de acceso al medio sobre los demás host.

- PIFS = SIFS + 1 slot = 78 µs.

- *DIFS:* DCF Intertrama Space. Usado por hosts operando bajo la función DCF para transmitir tramas de datos. DIFS = PIFS + 1 slot = 128 µs.

- *EIFS:* Extended Intertrama Space. El EIFS está definido para proveer suficiente tiempo para otro host para reconocer que fue, para este host, una incorrecta recepción de la trama antes de que este host comience la transmisión.

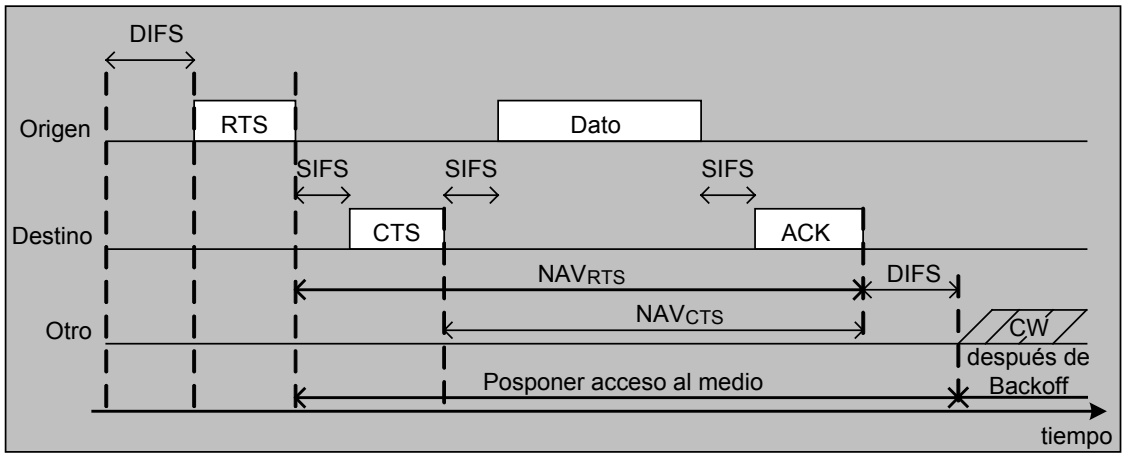


Figura 25. Escena de los campos RTS/CTS/Dato/ACK y NAV.

La Figura 25 indica el NAV para el host que genera la trama RTS, mientras el host receptor recibe la trama CTS, resultando la barra más baja del NAV como se muestra (exceptuando el host para el cual la trama RTS fue dirigida).

1.2.1.5.3.2 Los Servicios

Una red inalámbrica está formada por dos hosts o cientos de ellos. Para que un host pueda comunicarse de manera inalámbrica, necesita que se le instale un adaptador de red. Un adaptador de red es un equipo de radio (con transmisor, receptor y antena) que puede ser insertado o conectado a un host. Aparte de los adaptadores de red, las redes inalámbricas pueden disponer también de unos equipos que reciben el nombre de Puntos

de Acceso. Un AP es como una estación base utilizada para administrar las comunicaciones entre los distintos hosts.

De lo anterior, las redes inalámbricas IEEE 802.11 están formadas por hosts y puntos de acceso y ambos reciben el nombre de estaciones. La subcapa MAC define como las estaciones acceden al medio mediante lo que se llama servicios de estaciones. De la misma forma, define cómo los puntos de acceso administran la comunicación mediante lo que se llama servicios de distribución.

Los servicios de estación de la subcapa MAC son los siguientes:

- *Autentificación.* Comprueba la identidad de una estación y la autoriza para asociarse. En una red cableada lo que identifica a un host como parte de la red es el hecho de estar conectado físicamente a ella. En una red inalámbrica no existe la conexión física, por lo que, para saber si un host forma o no parte de la red, hay que comprobar su identidad antes de autorizar su asociación con el resto de la red.

- *Desautenticación.* Cancela una autenticación existente. Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.
- *Privacidad.* Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP (Wired Equivalency Protocol, Protocolo de Equivalencia con Red Cableada). Este algoritmo pretende emular el nivel de seguridad que se tiene en las redes cableadas.

- *Entrega de datos.* Facilita la transferencia de datos entre estaciones.

Por su lado, los servicios de distribución son estos otros:

- Asociación. Para que un host pueda comunicarse con otros hosts a través del AP, debe primero estar asociado a dicho AP. Asociación significa asignación del host al punto de acceso haciendo que éste sea el responsable de la distribución de los datos a, y desde, dicho host. En las redes con más de un punto de acceso, un host sólo puede estar asociado a un punto de acceso simultáneamente.

- Desasociación. Cancela una asociación existente, bien porque el host sale del área de cobertura del punto de acceso, o porque el punto de acceso termina la conexión.

- Reasociación. Transfiere una asociación entre dos puntos de acceso. Cuando un host se mueve del área de cobertura de un punto de acceso a la de otro, su asociación cambia pasa a depender de este último.

- Distribución. Cuando se transfieren datos de un host a otro, el servicio de distribución se asegura de que los datos alcanzan su destino.

- Integración. Facilita la transferencia de datos entre la red inalámbrica IEEE 802.11 y cualquier otra red, por ejemplo, Internet o Ethernet.

Servicio MAC	Definición	Tipo de Estación
Autentificación	Comprueba la identidad de una estación y la autoriza para asociarse	Hosts y puntos de acceso
Desautentificación	Cancela una autentificación existente	Hosts y puntos de acceso
Asociación	Asigna el host al punto de acceso	Puntos de acceso
Desasociación	Cancela una asociación existente	Puntos de acceso
Reasociación	Transfiere una asociación entre dos puntos de acceso	Puntos de acceso
Privacidad	Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP	Hosts y puntos de acceso
Distribución	Asegura la transferencia de datos entre estaciones de distintos puntos de acceso	Puntos de acceso
Entrega de datos	Facilita la transferencia de tatos entre estaciones	Hosts y puntos de acceso
Integración	Facilita la transferencia de datos entre redes Wi-Fi y no Wi-Fi	Puntos de acceso

Tabla 12. Servicios de la Subcapa MAC.

Los puntos de acceso utilizan tanto los servicios de estaciones como los servicios de distribución, mientras que los hosts solo utilizan los servicios de estaciones.

1.2.1.5.3.3 La Gestión

Tanto la capa física como la subcapa MAC están divididas en capacidades de gestión y de transferencia de datos. Lo que se conoce como PLME (PHY Layer Management Entity, Entidad de Gestión de la Capa Física) es quien se encarga de la gestión de la capa física, mientras que lo que se conoce como MLME (MAC Layer Management Entity, Entidad de Gestión de la Capa MAC) es quien se encarga de la gestión de la capa MAC. PLME y MLME intercambian información a través de MIB (Management Information Base, Base de Datos de la Información de Gestión). Ésta es una base de datos de las características físicas (velocidad de transmisión, niveles de potencia, tipo de antena, etc.) de las estaciones.

1.2.1.5.3.4 El Flujo de Datos

Los datos que se van a transmitir por el medio radioeléctrico proceden de las capas superiores (formato IP) y se la pasan a la subcapa LLC. La subcapa LLC le pasa estos datos a la subcapa MAC, quien, a su vez, se los pasa a la capa física para su emisión.

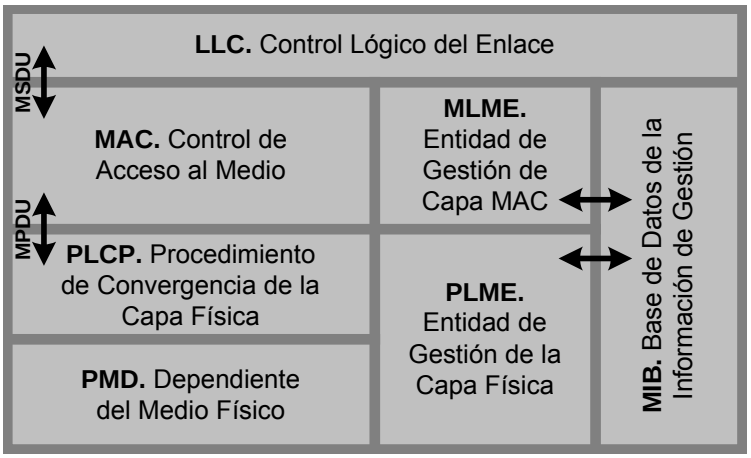


Figura 26. Interfaces de la subcapa MAC y capa física.

Los paquetes de datos que se intercambian entre las subcapas LLC y MAC se conocen como MSDU (MAC Service Data Unit, Unidad de Datos del Servicio MAC), mientras que los paquetes de datos que se intercambiaban entre la subcapa MAC y capa física reciben el nombre de MPDU (MAC Protocol Data Unit, Unidad de Datos del Protocolo MAC). En la capa física, quien recibe estos datos es PLCP, quien es responsable de convertir los datos MPDU a un formato compatible con el medio físico.

1.2.1.5.4 Trama IEEE 802.11

Además, la función de acceso al medio y del control de flujo provisto, la subcapa MAC de IEEE 802.11 cumple la función de segmentación y reensamblaje de tramas. Debido a que IEEE 802.11 funciona en conjunto con las redes Ethernet tradicionales, no tiene sentido utilizar una WLAN que no sea capaz de manejar tramas de hasta 1518 bytes. Pero dado que el medio físico de una WLAN es bastante propenso a errores, resulta conveniente manejar tramas más pequeñas para disminuir el efecto de las sucesivas retransmisiones. Por esta razón, el comité implanto la segmentación de carga útil de una trama a nivel de enlace tradicional, en tramas más pequeñas, las que tienen cada una un encabezado de nivel 2 y que deben ser confirmados positivamente para poder enviar el siguiente fragmento de la trama. En el receptor se lleva a cabo la función inversa y se vuelve a ensamblar el dato.

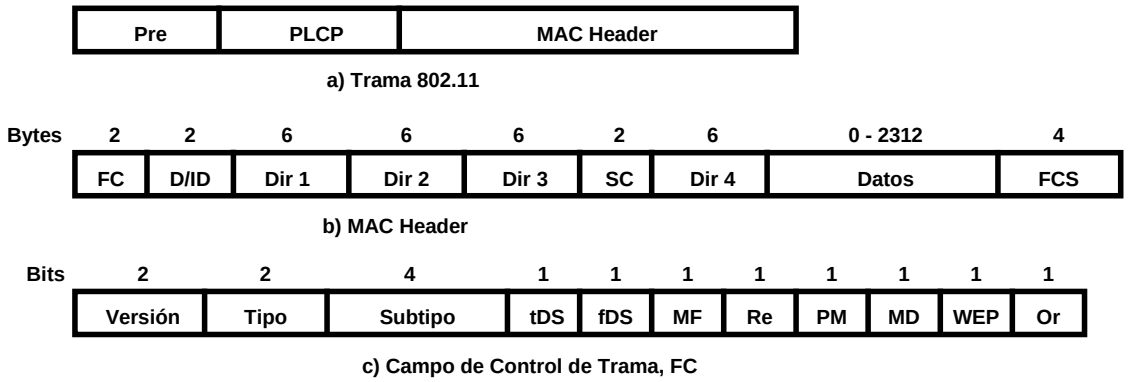


Figura 27. Formato de una trama de datos IEEE 802.11: a) Formato general, b) Campo MAC Header y c) Campo de control de trama.

La figura 27a, muestra el formato de la trama IEEE 802.11. La descripción de los campos del formato general es la siguiente:

Preámbulo: 96 bits de sincronización, de los cuales los primeros 80 son una serie de 1 y 0 alternados, y los últimos 16 delimitan el inicio de la trama con el patrón 0000 1100 1011 1101.

PLCP: Encabezado que contiene información que le sirve a la capa física para decodificar la trama. Contiene el largo del campo de datos además de un CRC para el encabezado.

MAC Header: El formato de la trama MAC comprende un juego de campos con la información típica del nivel de enlace. Es detallado a continuación.

Descripción de los campos de la trama MAC Header, de la figura 27b.

Trama Control (FC, Trama de Control): 2 Bytes usados para múltiples funciones de control.

Duration/ID (D/ID, Identificador de Duración): 2 Bytes que cumplen doble función. Si se trata de una trama de control para el ahorro de energía, entonces, el campo indica el identificador de la estación. Si es otro tipo de trama, indica el valor usado para el cálculo del NAV.

Dirección 1 (Dir 1): 6 Bytes. Corresponde siempre a la dirección destino. Si el bit toDS está activo corresponde a la dirección del AP, en caso contrario corresponde a un usuario wireless destino. Ver tabla 13.

Dirección 2 (Dir 2): 6 Bytes. Corresponde siempre a la dirección origen. Si el bit fromDS está activo corresponde a la dirección del AP, en caso contrario corresponde a un usuario wireless origen. Ver tabla 13.

Dirección 3 (Dir 3): 6 Bytes. La mayor cantidad de veces corresponde a la dirección “faltante”. Si la trama tiene el bit fromDS en 1 corresponde a la dirección

original fuente. Si la trama tiene el bit toDS en 1 corresponde a la dirección destino. Ver Tabla 13.

Sequence Control (SC, Control de Secuencia): 2 Bytes que permiten numerar la secuencia y los segmentos de una trama, en el caso de que se divida una trama.

Dirección 4 (Dir 4): 6 Bytes. Útil en el caso especial en que se use el DS (Distribution System, Sistema de Distribución) y la trama deba transferirse desde un AP a otro (similar a un esquema de telefonía celular) que corresponde al caso en que los bits toDS y fromDS estén en 1. En este caso, los campos Dirección 3 y Dirección 4 contienen las direcciones fuente y origen de los hosts. Ver tabla 13.

toDS	FromDS	Dirección 1	Dirección 2	Dirección 3	Dirección 4	Significado
0	0	DA	SA	BSSID	N/A	Datos desde un host a otro dentro del BSS. Datos de control
1	0	DA	BSSID	SA	N/A	Datos destinados al DS
0	1	BSSID	SA	DA	N/A	Datos provenientes del DS
1	1	RA	TA	DA	SA	Tramas que van de un AP a otro AP (WDS)

Tabla 13. Resumen del uso de los campos de direcciones en una trama IEEE 802.11.

Datos: Campo que contiene los datos dirigidos a capas superiores.

FCS: 4 Bytes que contiene 32-bit CRC. El FCS es calculado sobre los campos del MAC Header y el campo de datos, para asegurar que la trama llegó en buen estado.

La figura 19c ilustra el detalle de la trama de control, que corresponde al primer campo de la trama MAC Header:

Versión: 2 bits para indicar la versión del protocolo. Actualmente el valor que se coloca es 00. Los demás valores están reservados. El nivel de la revisión sólo se incrementará cuando una incompatibilidad fundamental existe entre una nueva revisión y la edición anterior de la norma.

Tipo: 2 bits que en conjunto con el campo Subtipo definen la función de la trama, es decir, si la trama es de control, de datos, de administración o reservado. Ver tabla 9.

Subtipo: 4 bits que en conjunto con el campo Tipo definen la función de la trama, es decir, si la trama es de control, de datos, de administración o reservado. Ver tabla 9.

toDS (tDS, Para el Sistema de Distribución): 1 bit que es puesto en 1 para indicar el destino de tipo de tramas de datos a el DS. Éstas incluyen todos los tipos de

tramas de datos enviados por un host asociado a un AP. Es puesto en cero en todas las otras tramas. Ver tabla 8.

fromDS (fDS, Proveniente del Sistema de Distribución): 1 bit que es puesto en 1 para indicar el tipo de tramas de datos provenientes de un DS. Es puesto en cero en todas las otras tramas. Ver tabla 13.

More Fragments (MF, Más Fragmentos): 1 bit que es puesto en 1 para indicar que los tipos de tramas de datos o de administración se han dividido y existen más fragmentos a continuación. Es puesto en cero en todas las otras tramas.

Retry (Re, Reintento): 1 bit que es puesto en 1 para indicar que los tipos de tramas de datos o de administración han sido retransmitidas de alguna trama anterior. Es puesto en cero en todas las otras tramas. Un host receptor utiliza esta indicación para ayudar al proceso de eliminar tramas duplicadas.

Power Management (PM, Administración de Potencia): 1 bit que establece el modo de operación una vez finalizada la transmisión de una trama. Los estados pueden ser ahorro de energía o activo. Está en 1 cuando opera el modo de ahorro de energía.

More Data (MD): 1 bit usado para indicarle al AP que existen más tramas almacenados en él.

WEP (Wired Equivalency Protocol): 1 bit que es puesto en 1 para indicar que el campo de datos está encriptado.

Order (Or): 1 bit que es puesto en 1 para cualquier tipo de tramas de datos que contenga un MSDU o fragmentos de éste, el cual está transfiriéndose usando la clase de servicio Strictly-Ordered (Estrictamente Ordenado).

Tipo de valor b3 b2	Tipo de descripción	Valor de subtipo b7 b6 b5 b4	Subtipo de descripción
00	Administración	0000	Petición de asociación
00	Administración	0001	Respuesta de asociación
00	Administración	0010	Petición de reasociación
00	Administración	0011	Respuesta de reasociación
00	Administración	0100	Petición de prueba
00	Administración	0101	Respuesta de prueba
00	Administración	0110-0111	Reservado
00	Administración	1000	Beacon
00	Administración	1001	Mensaje de indicación de anuncio de tráfico
00	Administración	1010	Desasociación
00	Administración	1011	Autenticación
00	Administración	1100	Desautenticación
00	Administración	1101-1111	Reservado
01	Control	0000-1001	Reservado
01	Control	1010	Ahorro de energía - Poll (PS, Power Save)
01	Control	1011	Envío de petición (RTS, Request to Send)
01	Control	1100	Listo para Envío (CTS, Clear to Send)
01	Control	1101	Conocimiento (ACK, Acknowledgment)
01	Control	1110	Libre Contención – Final (CF, Contention Free – End)
01	Control	1111	CF-END + CF-ACK
10	Datos	0000	Datos
10	Datos	0001	Datos + CF-ACK
10	Datos	0010	Datos + CF-Poll
10	Datos	0011	Datos + CF-ACK + CF-Poll
10	Datos	0100	Función nula (sin datos)
10	Datos	0101	CF-ACK (sin datos)
10	Datos	0110	CF-Poll (sin datos)
10	Datos	0111	CF-ACK + CF-Poll (sin datos)
10	Datos	1000-1111	Reservado
11	Reservado	0000-1111	Reservado

Tabla 14. Tabla de combinaciones del campo tipo y subtipo.

El formato de la trama RTS, se muestra en la figura 20a, está formado por 5 campos. El campo RA es la dirección del host destino de la trama y el campo TA es la dirección del host origen de la trama. El valor de Duración es el tiempo, en μs, requerido para transmitir tramas de datos o de administración pendientes, más una trama CTS, más una trama ACK, más tres intervalos SIFS. Si la duración calculada incluye una fracción de microsegundo, el valor es redondeado al siguiente número entero superior. Los campos FC y FCS ya han sido descritos anteriormente.

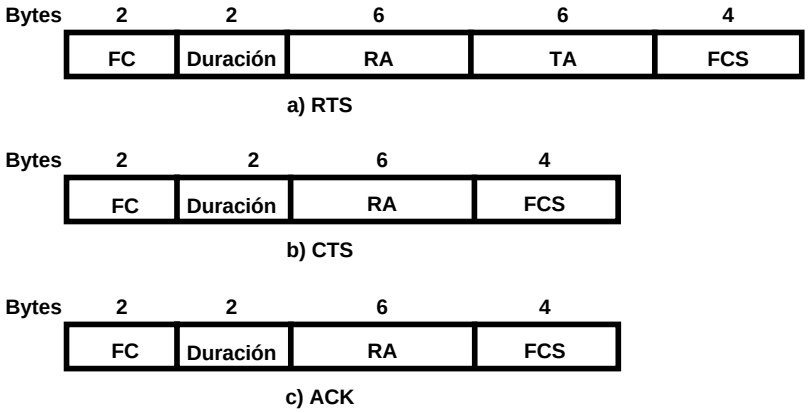


Figura 28. Formato de las tramas: a) RTS, b) CTS y c) ACK.

El formato de la trama CTS, se muestra en la figura 28b, está formado por 4 campos. El campo RA de la trama CTS es copiado del campo TA de la trama RST, ya que el CTS es una respuesta del RTS. El valor de Duración es el valor obtenido del campo Duración de la trama RTS, menos el tiempo, en microsegundos, requerido para transmitir la trama CTS y los intervalos SIFS. Si la duración calculada incluye una fracción de microsegundo, el valor es redondeado al siguiente número entero superior. Los campos FC y FCS ya han sido descritos anteriormente.

El formato de la trama ACK, se muestra en la figura 28c, está formado por 4 campos. El campo RA de la trama ACK es copiado del campo de Dirección 2 de los datos anteriores dirigidos inmediatamente, de administración o la trama de control PS-Poll. Si el campo More Fragments fue enviado en 0 en la trama de control de los datos anteriores dirigidos inmediatamente, de una trama administración, el valor de Duración es ajustado en 0. Si el campo More Fragments fue enviado en 1 en la trama de control de los datos anteriores dirigidos inmediatamente o de una trama administración, el valor de Duración es el valor obtenido del campo de Duración de los datos anteriores dirigidos inmediatamente o de una trama administración, menos el tiempo, en microsegundos, requeridos para transmitir la trama ACK y los intervalos SIFS. Si la duración calculada incluye una fracción de microsegundo, el valor es redondeado al siguiente número entero superior. Los campos FC y FCS ya han sido descritos anteriormente.

1.2.1.5.5 La Estructura de Red

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11 y, por tanto, Wi-Fi contempla tres topologías distintas:

- *IBSS* (Independent Basic Service Set, Conjunto de Servicios Básicos Independientes). Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre los distintos hosts que forman la red. En este caso no existe ningún host principal que coordine al grupo, no existe punto de acceso. Todas las comunicaciones son directas entre dos o más hosts del grupo. A esta modalidad se le conoce también como *ad hoc, independiente o peer to peer* (igual a igual).

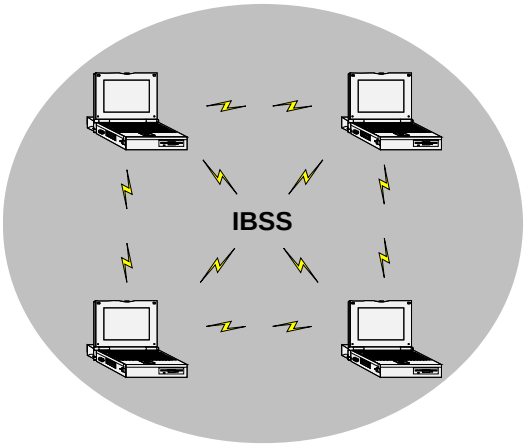


Figura 29. Estructura de red Ad hoc.

➢ *BSS* (Basic Service Set, Conjunto de Servicios Básicos). En esta modalidad se añade un AP que realiza las funciones de coordinación centralizada de la comunicación entre los distintos hosts de la red. Los puntos de acceso tienen funciones de búfer (memoria de almacenamiento intermedio) y de gateway con otras redes. A los equipos que realizan la función de gateway con otras redes externas se les conoce como portales. A la modalidad BSS también se le conoce como modo infraestructura.

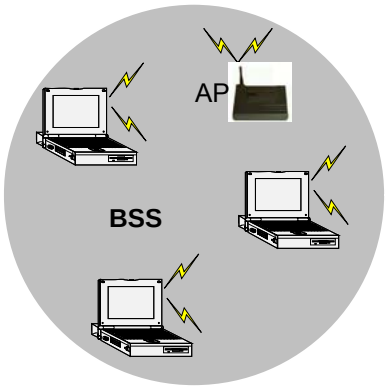


Figura 30. Estructura de red BSS.

➢ *ESS* (Extended Service Set, Conjunto de Servicios Extendido). Esta modalidad permite crear una red inalámbrica formada por más de un AP. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

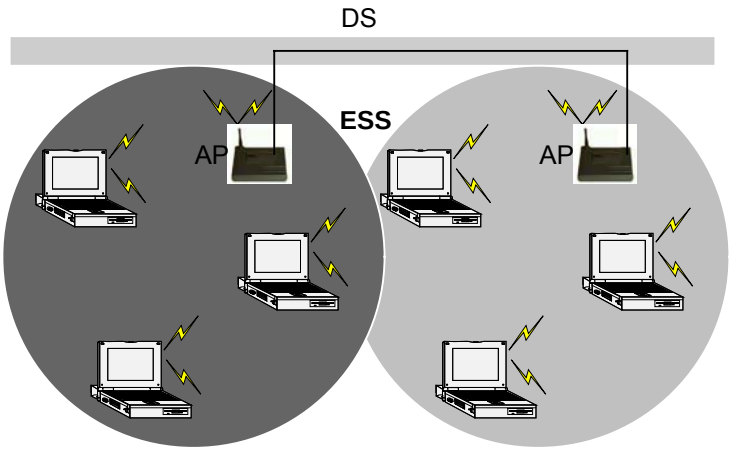


Figura 31. Estructura de red ESS.

En las modalidades BSS y ESS todas las comunicaciones pasan por los AP. Aunque dos hosts estén situados uno junto al otro, la comunicación entre ellos pasará por el AP al que estén asociados. Esto quiere decir que un host no puede estar configurado para funcionar en la modalidad ad hoc (IBSS) y de infraestructura (BSS) a la vez.

Veamos de manera específica como funciona el direccionamiento en modo ESS. El caso más complejo de direccionamiento se produce cuando un host quiere transmitir a otro ubicado en un BSS diferente. En este caso, los campos ToDS = FromDS = 1 y las direcciones de cada uno de los componentes por los que pasa la trama toman el siguiente valor de la trama MAC Header, quedando el campo Dirección 1 como el host destino, el campo Dirección 2 será la del punto de acceso final, el campo Dirección 3 sería la del punto de acceso origen, y por último, el campo Dirección 4 sería la del host origen. En la figura 31, podemos ver un ejemplo de este caso donde la transmisión se realiza del host A al host H en BSSs diferentes.

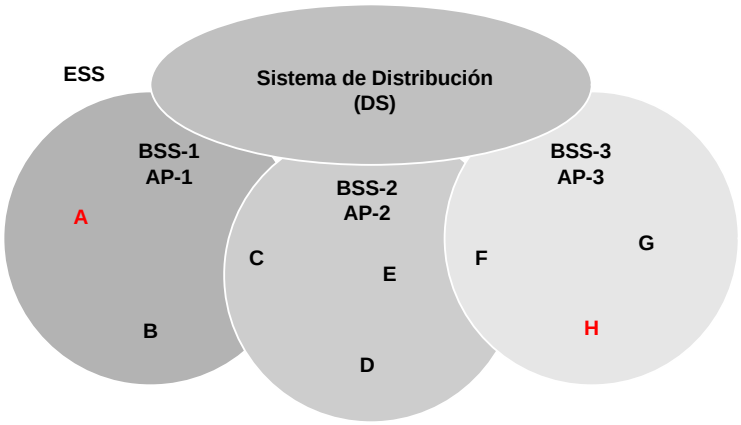


Figura 32. Transmisión del host A al host H.

1.2.1.5.6 Instalar una Red WLAN

Cada punto de acceso dispone de un área de cobertura. Un área de cobertura es la zona dentro de la cual cualquier host puede comunicarse con el punto de acceso de forma inalámbrica. El punto de acceso es el equipo del que dependen todas las comunicaciones y desde el que se puede gestionar toda la red. El tamaño del área de cobertura depende de los distintos factores, como son:

- Localización del punto de acceso
- Obstáculos entre el punto de acceso y el host
- Interferencias radioeléctricas
- Tipos de antenas utilizadas (potencia, patrón de radiación, etc.)

Si se sitúan distintos puntos de acceso complementando sus coberturas, se puede llegar a crear una red local inalámbrica con un área de servicio considerable.

La colocación de los puntos de acceso tiene una gran base técnica, pero también tiene un gran componente artístico. Esto se debe a que cualquier cosa del entorno (muebles, estantería, paredes, fenómenos atmosféricos, metales, árboles, etc.) puede afectar la propagación de las ondas electromagnéticas y, generalmente, no es posible realizar un estudio teórico de la propagación de las ondas electromagnéticas en nuestro entorno (EMI). Por ello, teniendo presente lo que afecta a la propagación, la colocación de los puntos de acceso suele basarse en el método de prueba y error.

El método de prueba y error consiste en realizar una inspección previa en el sitio donde se instalarán los puntos de acceso, decidir los lugares de los puntos de acceso basados en esta primera inspección, hacer pruebas de cobertura con la ayuda de una Laptop y recolocar los puntos de acceso hasta situarlos en su posición idónea de acuerdo al área que nos interesa cubrir.

En cualquier caso, antes de proceder a instalar los puntos de acceso, es necesario tener claro el área de cobertura que se desea cubrir, cuántos usuarios concurrentes habrá en cada área y qué tipo de usuario (802.11a, 802.11b ó 802.11g) se le dará servicio en cada o todas las áreas. Un área muy congestionada puede necesitar más de un punto de acceso.

1.2.1.5.6.1 Análisis Previo

En las redes pequeñas, hay poco que analizar: se coloca el punto de acceso en el lugar más cómodo y se comprueba si cubre las expectativas. En el peor de los casos, bastará con hacer un par de intentos de colocación antes de llegar a la posición óptima.

El tema se complica un poco cuando se necesita cubrir una gran extensión, por ejemplo, un campus universitario. En estos casos, para conseguir la mayor eficiencia, no basta con situar los puntos de acceso donde mejor parezca. Tampoco hay que confiar exclusivamente en el sistema de prueba y error. En estos casos es recomendable realizar un estudio más estructurado. Esto quiere decir, antes de comenzar a colocar puntos de acceso por paredes y techos, nos hará falta responder a algunas preguntas como las siguientes:

- ¿Con cuántos usuarios va a contar la red y de qué tipo (802.11a, 802.11b ó 802.11g)?
- ¿Qué área se pretende cubrir?
- ¿Qué inconvenientes puede presentar el entorno desde el punto de vista de la cobertura radioeléctrica (interferencias)?
- ¿Cuál será la concentración de usuarios (usuarios concurrentes en la misma zona)?
- ¿Qué perfil de movilidad tendrán los usuarios?
- ¿Qué equipamiento será necesario (adaptadores de red, puntos de acceso, etc.)?
- ¿Cómo se interconectarán los puntos de acceso entre sí?
- ¿Qué nivel de seguridad se necesitará?
- ¿Cómo se interconectara la red inalámbrica a la red cableada o Internet?
- ¿Cuánto presupuesto se destinará a la red inalámbrica?

Dicho de otra forma, cuanto mayor sea la red, tanto en extensión como en número de usuarios, mayor será la necesidad de realizar un análisis previo que nos permita conocer en detalle las necesidades y los recursos con los que se cuenta.

El análisis previo supone simplemente definir las necesidades, analizar el terreno, estudiar los posibles inconvenientes y calcular los recursos. El tener una idea clara de estos conceptos ayudará grandemente a obtener una red adecuada y eficaz.

Los pasos a dar son los siguientes:

1. *Determinar las necesidades.* Se parte de que se conoce exactamente el área que se pretende cubrir y los usuarios de la red.

2. *Hacer un esquema de cobertura.* Dibujar un esquema o plano donde se especifiquen las áreas a cubrir y las necesidades en cada área.

3. *Decidir las áreas de movilidad.* Habrá áreas en las que baste tener servicio, mientras que en otras se necesitará garantizar además que el servicio no se corta cuando se desplaza el usuario. Se tiene, por tanto, que determinar las áreas con uno y otro tipo de movilidades. Es posible que este último aspecto afecte la distribución de los puntos de acceso. Las opciones son las siguientes:

   - *Lugares con cobertura.* Son aquellas zonas que tiene que estar cubiertas porque hay usuarios que necesitan conectarse a la red desde allí. Incluso puede haber zonas que necesitan estar cubiertas muy esporádicamente. En este caso, pueden disponerse de puntos de acceso que ocasionalmente puedan estar situados en lugares distintos.

   - *Lugares por los que desplazarse (roaming).* Son las zonas por las que se desplazan los usuarios haciendo uso de la conexión. Estas áreas deben garantizar una continuidad del servicio aunque los usuarios estén en movimiento.

4. *Estudiar la cobertura real.* Una vez descritas las necesidades, se puede hacer una comprobación práctica de la cobertura. Se instala una tarjeta inalámbrica en una Laptop, se va situando el punto de acceso y la Laptop en distintos sitios y se va comprobando el nivel de la señal dentro de las áreas a cubrir. Esto nos da una

idea de donde situar mejor los puntos de acceso. Para cada localización se debe de comprobar tanto el alcance, como la respuesta (velocidad máxima conseguida). Para comprobar el alcance, basta con desplazarse y ver que la conexión sigue establecida. Para comprobar la calidad de respuesta, se pueden realizar transferencias de archivos y ver la velocidad de transmisión de datos. En las zonas con interferencias se notará que la velocidad de transferencia puede llegar a ser realmente baja. Por cierto, la mayoría de equipos Wi-Fi incluyen un software de utilidades que permiten verificar la calidad de la señal (intensidad de la señal, ruidos, velocidad de transmisión, etc.). Este software puede resultar muy útil para estudiar la cobertura real. Hay que tener siempre en cuenta que, en general, el mejor punto para colocar un punto de acceso será el centro y en posición elevada del área de cobertura. En lugares repletos de obstáculos, como muebles, librerías, estantes, archiveros, etc., se consiguen coberturas inferiores que en lugares abiertos. Definitivamente, hay que evitar esconder el punto de acceso dentro de los típicos cubículos separadores de las oficinas, en armarios o ponerlos cerca de objetos de metal.

5. *Identificar Interferencias.* El entorno radioeléctrico está sujeto a la presencia de interferencias. Las interferencias pueden bajar el rendimiento del sistema; por ello, es importante identificar las posibles fuentes de interferencias. Generalmente, estas fuentes proceden de dispositivos como hornos de microondas, teléfonos inalámbricos, dispositivos bluetooth, motores (de ascensores, por ejemplo) o alarmas. El impacto de estas fuentes de interferencia se puede comprobar haciendo pruebas de transferencia con los dispositivos encendidos y apagados. En los lugares con interferencias donde nos se pueda eliminar la fuente y sea necesario la cobertura, se puede colocar puntos de acceso adicionales (en distintos canales).

6. *Hacer una instalación de prueba.* Hasta este momento, se tiene una idea muy clara de las condiciones del entorno. No obstante, antes de lanzarse a instalar todos los puntos de acceso, conviene hacer una primera instalación de prueba donde sólo se conecten unos cuantos usuarios. Esto puede ayudar a detectar posibles problemas de desplazamiento o de congestión por interferencias.

7. *Realizar la comprobación final.* Una vez hechas todas las comprobaciones anteriores, se contará con todos los datos necesarios para hacer la instalación: localización de los puntos de acceso, identificación de zonas muertas, modelo de funcionamiento del roaming, fuentes de interferencia, número y localización de los usuarios.

1.2.1.5.6.2 Cobertura

La cobertura de un punto de acceso puede variar entre los 30 y los 300 m dependiendo de las condiciones de visibilidad entre el emisor y el receptor y de las posibles interferencias que se pueda producir en la zona. En los espacios abiertos se consiguen los mayores alcances, mientras que en los lugares de interior con paredes y muebles se consiguen alcances muy reducidos. Esto quiere decir que los puntos de acceso no se pueden colocar con el único criterio del alcance teórico, comparar las tablas 15, 16, 17 y 18.

Por otro lado, la potencia de transmisión de un punto de acceso varía entre los 100 mW (límite máximo de acuerdo con la regulación europea) y 1 W (límite máximo de acuerdo con la regulación norteamericana). Evidentemente, a más potencia, mayor es el alcance. No obstante, no siempre interesa que un solo punto de acceso tenga una gran cobertura. Si lo que se pretende cubrir es, por ejemplo, una pequeña oficina o sala de reuniones, el disponer de una cobertura mucho mayor (llegando a la calle o a las oficinas vecinas) no tiene ningún interés y, sin embargo, se aumenta el riesgo de seguridad de la red. Por otro lado, cuando se intenta cubrir un área donde se concentran muchos usuarios, a menor cobertura de cada punto de acceso, más puntos de acceso serán necesarios para cubrir la misma área y mayor será el ancho de banda total disponible.

Velocidad de transmisión	**Distancia en interior**	**Distancia en exterior**
11 Mbps	50 m	270 m
5.5 Mbps	80 m	380 m
2 Mbps	130 m	430 m
1 Mbps	160 m	540 m

Tabla 15. Relación entre distancia y velocidad con un equipo 802.11b. Condiciones ideales.

Fabricante y Modelo	*AP Cisco Aironet 1200 (100 mW con 2.2 dBi de ganancia de la antena dipolo de diversidad)*		*Orinoco AP-500 (Proxym)*	
Velocidad de transmisión	Distancia en interior	Distancia en exterior	Distancia en interior	Distancia en exterior
11 Mbps	48 m	304 m	25 m	160 m
5.5 Mbps	67 m	-	35 m	270 m
2 Mbps	82 m	-	40 m	400 m
1 Mbps	124 m	610 m	50 m	550 m

Tabla 16. Relación entre distancia y velocidad con equipos 802.11b.

Fabricante y Modelo	*AP Cisco Aironet 1200 (30 mW con 2.2 dBi de ganancia de la antena dipolo de diversidad)*		*Orinoco AP-2000 11b/g Kit (Proxym)*	
Velocidad de transmisión	**Distancia en interior**	**Distancia en exterior**	**Distancia en interior**	**Distancia en exterior**
54 Mbps	27 m	76 m	15 m	40 m
48 Mbps	29 m	-	-	-
36 Mbps	30 m	-	-	-
24 Mbps	42 m	-	-	-
18 Mbps	54 m	183 m	-	-
12 Mbps	64 m	-	-	-
9 Mbps	76 m	-	-	-
6 Mbps	91 m	396 m	120 m	400 m

Tabla 17. Relación entre distancia y velocidad con equipos 802.11g.

Fabricante y Modelo	*AP Cisco Aironet 1200 (40 mW con 6 dBi de ganancia de la antena patch)*		*Orinoco AP-2000 11a Kit (Proxym). (dos antenas omnidireccionales de 5 dBi con una diversidad de 0-180 grados de articulación)*	
Velocidad de transmisión	**Distancia en interior**	**Distancia en exterior**	**Distancia en interior**	**Distancia en exterior**
54 Mbps	13 m	30 m	15 m	40 m
48 Mbps	15 m	-	-	-
36 Mbps	19 m	-	-	-
24 Mbps	26 m	-	-	-
18 Mbps	33 m	183 m	-	-
12 Mbps	39 m	-	-	-
9 Mbps	45 m	-	-	-
6 Mbps	50 m	304 m	120 m	400 m

Tabla 18. Relación entre distancia y velocidad con equipos 802.11a.

Por tanto, aunque un equipo pueda tener un gran alcance, siempre hay que configurarlo para que ofrezca la cobertura justa necesaria.

1.2.1.5.6.3 Roaming

Típicamente, las redes inalámbricas se implantan con equipos 802.11b, sin embargo, hoy día, es común implantarlas con 802.11g, que también abarca 802.11b, y 802.11a. Lo que nos debe dar el parámetro para seleccionar una sobre otra es el tipo de usuarios, aunque también podemos considerar la velocidad de transmisión, a los que se les piensa dar cobertura. Se debe de considerar que incluso se puede optar por una combinación de dos de éstas o todas. Esto puede solucionar muchas necesidades pero se puede volver muy complejo, ahora se verán algunas configuraciones.

Las redes 802.11b disponen de 11 canales de 11 Mbps cada uno. Cada canal viene identificado por un número del 1 al 11, recordemos que en México utilizamos 11 canales. Cada canal del protocolo DSSS de 802.11b necesita 22 MHz por canal para minimizar las interferencias entre canales. Como la banda de 2.4 GHz en la que trabaja 802.11b tiene un ancho de banda total de 80 MHz, esto quiere decir que en una misma zona solo puede coexistir tres canales (tres puntos de acceso) sin que haya interferencia entre canales.

En la figura 33, se muestra una distribución de canales en células hexagonales. Cada número de canal 802.11b corresponde con una frecuencia determinada. Por tanto, mientras más diferencia haya entre los números de canal, mayor diferencia habrá entre sus frecuencias. En una red con múltiples puntos de acceso es interesante tener en cuenta este detalle para intentar configurar a los puntos de acceso vecinos, no solamente con canales distintos (cosa imprescindible), sino que sus frecuencias estén lo más lejanas posible.

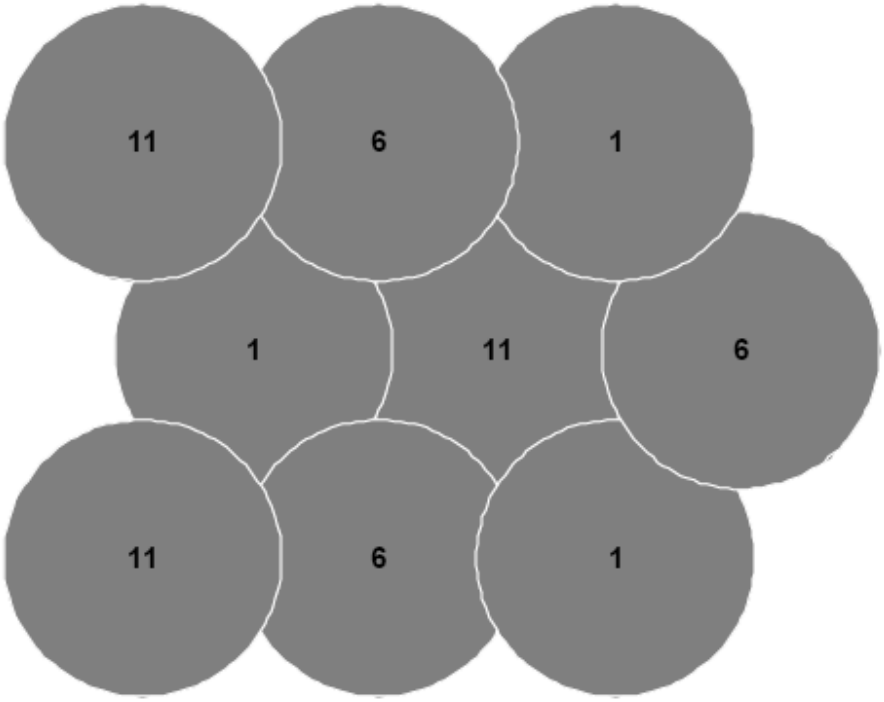


Figura 33. Distribución de canales en células hexagonales, 802.11b.

En teoría, con tan sólo tres frecuencias se podría cubrir cualquier área, por grande que ésta fuera, sin dejar zonas en sombra. Para ello, basta con imaginarse que cada punto de acceso dispone de un área de cobertura hexagonal (lo que también se conoce como célula). Como se dispone de 11 canales, una buena elección de canales sería el 1, 6 y 11. Esto nos dejaría una distancia de cuatro canales intermedios.

Canal	Frecuencia [MHz]	FCC (USA)	ETSI (Europa)	España	Francia	Japón
1	2412	x				X
2	2417	x				X
3	1422	x	x			X
4	1427	x	x			X
5	2432	x	x			X
6	2437	x	x			X
7	2442	x	x			X
8	2447	x	x			X
9	2452	x	x			X
10	2457	x	x	x	x	X
11	2462	x	x	x	x	X
12	2467		x		x	X
13	2472		x		x	X
14	2484					X

Tabla 19. Regulación de canales y frecuencias en distintos países para 802.11b.

En la asignación de canales a los puntos de acceso, hay que tener en cuenta que la propagación de las señales de radio se efectúa tanto horizontal como verticalmente. Esto quiere decir que, si existen dos plantas de un edificio cubiertas por distintos puntos de acceso, habría que comprobar que no se producen interferencias entre pisos.

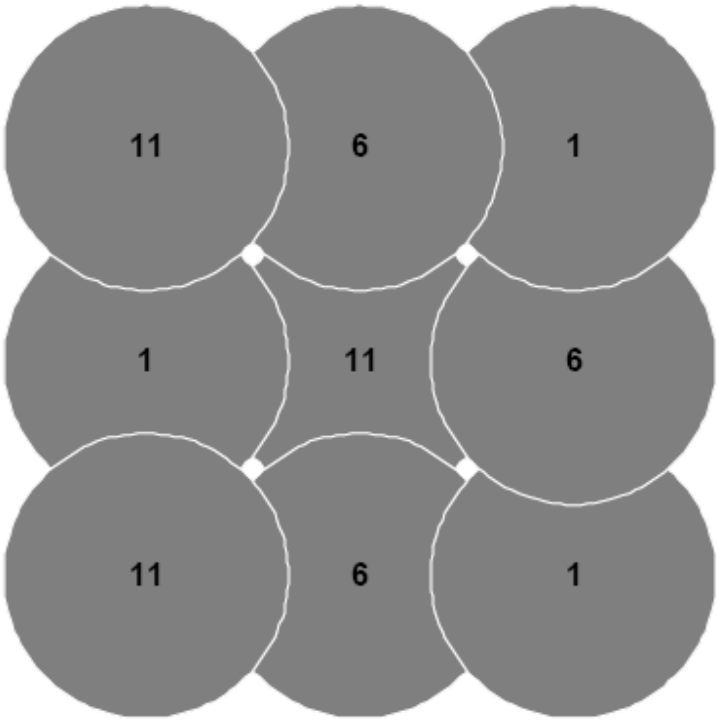


Figura 34. Distribución de canales en células cuadradas, 802.11b.

Dominio regulador	Banda [GHz]	Número de canales operando	Frecuencia central del canal [MHz]
FCC	U-NII banda baja (5.15-5.25)	36 40 44 48	5180 5200 5220 5240
FCC	U-NII banda media (5.25-5.35)	52 56 60 64	5260 5280 5300 5320
FCC	U-NII banda alta (5.725-5.825)	149 153 157 161	5745 5765 5785 5805

Tabla 20. Regulación de canales y frecuencias para 802.11a.

En las redes 802.11 a, las bandas baja y media permiten 8 canales en un total de 200 MHz de ancho de banda. La banda alta permite 4 canales en un total de 100 MHz de ancho de banda. El centro del extremo de los canales debe ser a una guarda de 30 MHz para las bandas baja y media, y 20 MHz para la banda alta.

En 802.11a no hay problema de traslape entre canales, basta con utilizar un canal diferente y listo. Aquí lo único que debemos poner atención es el país donde se implantara la red. En México se pueden utilizar hasta 8 canales aunque en otros países solo se permite utilizar 4, es decir, los equipos que se fabrican para cada país solamente se pueden configurar los canales que están regulados por cada organismo local. Ver tabla 16. Con esta norma podemos manejar los esquemas utilizados en 802.11b, aunque definitivamente por el tipo de cobertura, es mejor utilizar la distribución de canales en células hexagonales.

Canal	Frecuencia [MHz]	FCC (USA)	Singapore	Taiwan	Japón
36	5180	x	x		x
40	5200	x	x		x
44	5220	x	x		x
48	5240	x	x		x
52	5260	x		x	
56	5280	x		x	
60	5300	x		x	
64	5320	x		x	
149	5745				
153	5765				
157	5785				
161	5805				

Tabla 21. Regulación de canales y frecuencias en distintos países para 802.11a.

Para el diseño de una red inalámbrica de área local con la norma 802.11g se debe considerar los mismos parámetros que con 802.11b, a diferencia de que con 802.11g podemos obtener una velocidad de transmisión de hasta 54 Mbps y, además, abarcar la norma 802.11b. Por lo que el esquema en cuanto a la distribución puede ser de las que puede utilizar 802.11b, es decir, células hexagonales y células cuadradas.

Finalmente, se puede utilizar puntos de acceso que soporte las tres normas (802.11b, 802.11a y 802.11g), por lo que en una sola célula se puede tener cobertura para cualquier tipo de usuario y contar con roaming, solamente se tiene que considerar que el número de canales posibles sin que exista interferencia son 11, 8 canales que proporciona 802.11a y 3 canales que proporcionan 802.11bg. Estos tipos de puntos de acceso cuentan con dos ranuras para insertar dos adaptadores de red PCMCIA (Personal Computer Memory Card International Association, Asociación Internacional de Tarjetas de Memoria para Computadoras Personales) y se pueden instalar con diferentes normas, por ejemplo, con 802.11bg y 802.11a.

Canal	Frecuencia [MHz]	FCC (USA)	ETSI (Europa)	España	Francia	Japón
1	2412	x				x
2	2417	x				x
3	1422	x	x			x
4	1427	x	x			x
5	2432	x	x			x
6	2437	x	x			x
7	2442	x	x			x
8	2447	x	x			x
9	2452	x	x			x
10	2457	x	x	x	x	x
11	2462	x	x	x	x	x
12	2467		x		x	x
13	2472		x		x	x
14	2484					x

Tabla 22. Regulación de canales y frecuencias en distintos países para 802.11g.

Por otro lado, si lo que interesa es darle mayor ancho de banda a una célula, entonces se debe colocar dos adaptadores de red o puntos de acceso con la misma norma, por ejemplo, 802.11g para que aumente de 54 Mbps a 108 Mbps por célula (11 Mbps a 22 Mbps, para 802.11b) y esto se puede aumentar más si se colocara otro punto de acceso solo hay que recordar que en 802.11b solo permite traslapar 3 canales en una misma área de cobertura sin que exista interferencia, mientras que en 802.11a se pueden traslapar hasta 8 canales.

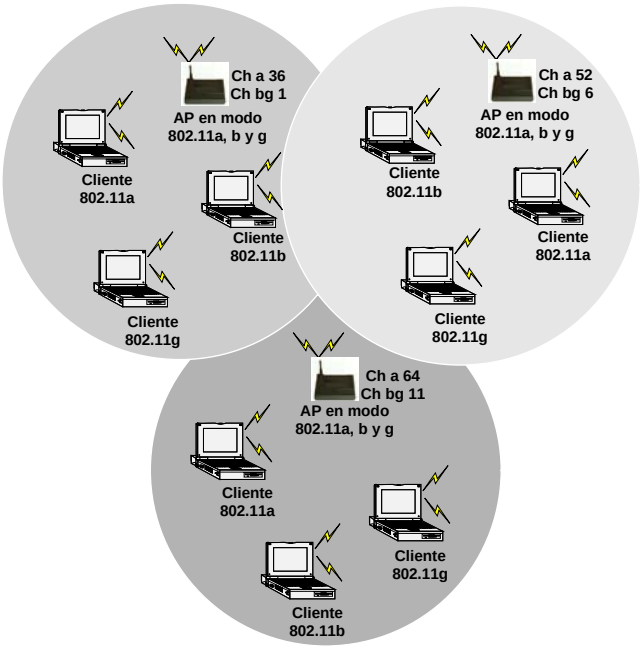


Figura 35. Distribución de canales en células hexagonales, con 802.11b, 802.11a y 802.11g.

1.2.1.5.7 Seguridad

Parte del diseño de una red es precisamente la seguridad, ya que depende si se diseña una red pública o privada, independientemente del tipo de red, no existe ningún sistema de seguridad que sea absolutamente impenetrable. El objetivo de cualquier sistema de seguridad es permitir el acceso a cualquier persona autorizada e impedírselo a cualquier otra. Sin embargo, el simple hecho de que una persona pueda entrar, aunque sea de forma autorizada, hace que el sistema deje de ser impenetrable. Si un intruso puede averiguar los pasos a seguir para entrar legalmente, conseguirá romper la barrera.

La seguridad es un riesgo tanto para las redes inalámbricas como para las cableadas. Hasta la fecha, todas las tecnologías informáticas que han ido apareciendo en el mercado han sido susceptibles, de una forma u otra, de ser violadas en su integridad, confidencialidad o autenticidad de los datos que contiene.

La norma IEEE 802.11 contempla tres mecanismos de seguridad:

- *SSID* (Service Set Identifier, Identificador de Conjunto de Servicios) es un código alfanumérico que se configura en cada host y punto de acceso que forma parte de la red. Este código puede ser utilizado como una simple contraseña entre el host y el punto de acceso o como un identificador del emplazamiento del emisor en una red pública. Existen puntos de acceso que permiten que se les deshabilite el sistema SSID. Lo cierto es que este sistema no garantiza la seguridad, ya que los códigos SSID son emitidos en forma de texto sin codificar. Cualquier receptor con el software adecuado puede averiguar estos datos, de hecho, Windows XP incluye un programa que es capaz de detectar automáticamente estos códigos y mostrarle al usuario la lista de redes disponibles (lista SSID) detectadas para que el usuario elija con cual conectarse.

- *Lista de direcciones MAC.* Se puede generar una lista de direcciones MAC y limitar el acceso a la red a aquellos ordenadores contemplados en la lista. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (en sistema numérico hexadecimal), por ejemplo, 12-AB-56-78-90-FE, e identifican a la tarjeta de los adaptadores de red. Las direcciones MAC nos son modificables por el usuario. No obstante, es cierto que estas direcciones se transmiten en forma de texto sin codificar y, por tanto, son fácilmente leíbles con un receptor adecuado. Un intruso experimentado podría leer una dirección correcta, configurársela a su host y acceder a la red sin problemas.

- *WEP.* La última medida de seguridad de Wi-Fi consiste en el algoritmo de cifrado WEP (Wired Equivalency Protocol, Protocolo de Equivalencia con Red Cableada). Con este sistema se cifran todos los datos que se intercambian entre los hosts y los puntos de acceso. WEP utiliza el algoritmo de cifrado PRNG (Pseudorandom Number Generation, Generación de Números Pseudoaleatorios) RC4 desarrollado en 1987 por RSA Data Security.

1.2.1.5.7.1 Las debilidades de 802.11

El sistema de cifrado WEP consiste en aplicar a los datos originales la operación XOR (O exclusiva) utilizando una clave generada de forma pseudoaleatoria. Los datos cifrados resultantes son los que se transmiten al medio.

Para generar la clave pseudoaleatoria, se utiliza una clave secreta definida por el propio usuario y un vector de inicialización (IV, Initialization Vector). La clave secreta es única y debe estar configurada en todos los hosts y puntos de acceso.

La longitud de los datos cifrados excede en cuatro caracteres a la longitud de los datos originales. Estos cuatro caracteres reciben el nombre de ICV (Integrity Check Vlaue, Valor de Comprobación de Integridad) y se utilizan para que el receptor pueda comprobar la integridad de la información recibida. Esto se hace mediante el algoritmo CRC-32.

Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta (distribuida a todos los hosts) para generar la semilla que permitirá descifrar los datos mediante el algoritmo PRNG.

Uno de los inconvenientes que tiene este sistema de cifrado es que la clave secreta es estática. Una vez asignada, se configura en cada host (por el administrador de red o por el usuario) y permanece invariable hasta que se vuelva a repetir este proceso manualmente. Por otro lado, el IV se trasmite en abierto a todos los hosts. El IV si cambia.

Se han hecho muchos estudios que demuestran que las redes inalámbricas IEEE 802.11 no gozan de altos niveles de seguridad. De acuerdo a un estudio realizado por un equipo de especialistas en seguridad de la Universidad de California en Berkeley (el ISAAC, Internet Security, Applications, Authentication and Cryptography) en enero de 2001, se hace referencia a cuatro tipos de ataques posibles contra WEP:

1. El primero hacia posible descifrar un mensaje basado en la fragilidad del IV (vector de inicialización de sólo 24 bits) y en la actualización de códigos estáticos.
2. El segundo ataque posibilitaría crear mensajes utilizando los mensajes existentes.
3. El tercer ataque permitiría descifrar la información contenida en las cabeceras de los paquetes. Con esto se podría reenviar los paquetes a otro host para allí descifrar su contenido.
4. El último ataque permitiría crear una tabla IV (vectores de inicialización) y claves permitiendo descifrar fácilmente todos los mensajes interceptados.

1.2.1.5.7.2 Las soluciones

En junio de 2001 el IEEE aprobó la norma 802.1x. Esta norma incluye un nuevo protocolo de seguridad conocido como EAP (Extensible Authentication Protocol, Protocolo de Autentificación Extensible). Este protocolo se utiliza para controlar el acceso de los usuarios a los puntos de acceso y autentificar sus comunicaciones.

EAP se utiliza también para poder hacer entrega segura de las claves de la sesión. Con EAP se pueden generar y distribuir automáticamente las claves WEP, eliminando la pesadez de un proceso manual que iba en detrimento de la seguridad.

802.1x está siendo cada vez más aceptado por la industria, por otro lado, el comité 802.11i está trabajando para que la norma 802.1x forme parte de la norma 802.11. Este comité 802.11i tiene el objetivo de mejorar la seguridad de las redes inalámbricas. Uno de

los puntos es el acceso y la autentificación (ahí es donde entra 802.1x), pero, además, incluye temas como una metodología del cifrado mejor que WEP, un mejor uso del IV (vector de inicialización) o protección contra los paquetes falsos, ataques de respuestas, etc. El primer borrador de IEEE 802.11i salió en enero de 2002.

Actualmente, la alianza Wi-Fi conjuntamente con el IEEE, ha sacado al mercado un nuevo sistema de seguridad para Wi-Fi conocido como WPA (Wi-Fi Protected Access, Acceso Wi-Fi Protegido).

WPA son unas especificaciones basadas en la norma 802.11i que mejora fuertemente el nivel de protección de datos y el control de acceso de las redes inalámbricas Wi-Fi. La gran ventaja de WPA es que pueden aplicarse a las redes Wi-Fi existentes y que es completamente compatible con el futuro sistema de seguridad integrada proporcionado por IEEE 802.11i.

WPA se puede instalar en los equipos Wi-Fi existentes de una forma tan sencilla como instalar un software en los equipos. Una vez instalado, el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados pueden acceder a la red y que los datos transmitidos permanecen completamente inaccesibles para cualquier usuario que no sea el destinatario.

WPA se empezó a implantar en la primera mitad del año 2003 y se espera que a corto plazo sustituya a WEP.

Las mayores ventajas que aporta WPA frente a WEP son dos:

- Mejoras en el cifrado de datos mediante TKIP (Temporal Key Integrity Protocol, Protocolo Temporal de Integridad de Clave). Este sistema asegura la confidencialidad de los datos.
- Autentificación de los usuarios mediante la norma 802.1x y EAP. Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red. No obstante, si se desea, permite el acceso de usuarios anónimos.

Actualmente, el IEEE está terminando de desarrollar las especificaciones de la norma 802.11i Como WPA salió antes que 802.11i, no puede seguir todas esta especificaciones. No obstante, lo que cubre actualmente WPA será completamente compatible con esta nueva norma. Se puede decir que WPA es un subconjunto de 802.11i. WPA ha tomado de 802.11i aquellas características que son ya comerciales, como 802.1x y TKIP, y ha dejado aparte aquellas otras características que 802.11i no tiene aún completamente definidas. Las características que no incluye WPA son básicamente la desautentificación segura, la desasociación, IBSS segura, cambios seguros de puntos de acceso, así como protocolos mejorados de cifrado como AES-CCMP. Uno de los inconvenientes mayores que incluyen algunas de estas características (no incluidas en WPA) es que requieren cambios en el hardware de los equipos Wi-Fi actuales. Por el contrario, todas las características que incluye WPA pueden ser actualizadas en los equipos Wi-Fi actuales mediante software o firmware.

La única manera de conseguir seguridad es manteniendo unas técnicas de protección adecuadas. Debe haber consciencia de que ningúna técnica de protección es eficaz al cien por ciento. Siempre existe riesgo aunque sea pequeño. No obstante, a más barreras de seguridad, menor será el riesgo.

1.3 Cableado Estructurado

Un sistema de cableado estructurado es la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor. Físicamente es una red de cable única y completa. Con combinaciones de alambre de cobre (pares trenzados sin blindar UTP), cables de fibra óptica, bloques de conexión, cables terminados en diferentes tipos de conectores y adaptadores. El cableado estructurado permite la administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos. Tales como el sistema de cableado de telecomunicaciones para edificios que presenta como característica saliente de ser general, es decir, soporta una amplia gama de productos de telecomunicaciones sin necesidad de ser modificado. Utilizando este concepto, resulta posible diseñar el cableado de un edificio con un conocimiento muy escaso de los productos de telecomunicaciones que luego se utilizarán sobre él.

Es crítico tener en cuenta la dinámica entre los protocolos de red, las prestaciones del cableado estructurado y la vida útil de la infraestructura de red. De la misma manera que sería un despilfarro la especificación de un cableado que no cumpla con los requerimientos actuales y futuros de la estrategia de sistemas de información de la compañía o de la institución, también sería un enorme gasto no justificado la sobre-especificación de un cableado estructurado debido a la mala interpretación de los requerimientos o aspectos de cada opción. Hasta el año 1993, las instalaciones de cable para comunicaciones internas de las empresas seguían exactamente las directivas del fabricante de la red instalada. Las instalaciones de voz (telefonía), datos (redes) e imagen (TV, seguridad, etc.) estaban separadas. Las redes de datos de cada departamento no se interconectaban. Cuando cambiaba una tecnología de red se debía cambiar todo el cableado.

Los motivos del Cableado Estructurado son los siguientes:

- La integración de las comunicaciones de computadoras, voz y vídeo en un mismo sistema multimedia.
- La aparición de normas que definen las condiciones de una instalación de cableado para cumplir unos mínimos de calidad.
- La necesidad de no dependencia del fabricante para las instalaciones. Cualquier ingeniero puede certificar una instalación para funcionar con redes multimedia.
- La necesidad de no dependencia de la tecnología de las redes. Las instalaciones dependen de parámetros físicos: distancias y ancho de banda.
- Los cambios físicos de los puestos de trabajo en la empresa no deben afectar a la instalación, así se debe hacer una planificación global del cableado.

1.3.1 Normas

El principal primer intento para definir una norma de cableado genérico para edificios comerciales empezó a mediados de los años ochenta. Aunque hubo esfuerzos anteriores a esas fechas para clasificar los diferentes sistemas, se basaban predominantemente en requerimientos particulares de proveedores específicos.

1.3.1.1 TIA/EIA 568-A: Norma de Cableado para Telecomunicaciones en Edificios Comerciales

En Julio de 1991, la "Electronic Industries Association/Telecommunications Industry Association" (Asociación de Industrias Electrónicas/Asociación de Industrias de Telecomunicaciones) publicó el documento ANSI/EIA/TIA-568, Norma de Cableado de Telecomunicaciones de Edificios Comerciales (*Commercial Building Telecommunications Wiring Standard*), para definir formalmente los requerimientos mecánicos y eléctricos del cable y los componentes que formaban los cableados de inmuebles en Estados Unidos. Esta Norma incluía especificaciones para cable trenzado sin blindaje (UTP - *Unshielded Twisted Pair*) de 100 Ω, de pares trenzados blindados de 150 Ω STP (*Shielded Swisted Pair*), coaxial de 50 Ω y fibra óptica de 62.5/125 µm. El cable de par trenzado y los elementos de conexión fueron especificados eléctricamente como componentes hasta 16 MHz.

El propósito de la norma EIA/TIA 568-A se describe en el documento de la siguiente forma: "Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante. También proporciona directivas para el diseño de productos de telecomunicaciones para empresas comerciales. El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado."

La norma EIA/TIA 568-A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para: Las topología, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características: Una distancia entre ellos de hasta 3 km, un espacio de oficinas de hasta 1,000,000 m^2, y una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean en sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a: Voz, Datos, Texto, Vídeo e Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

1.3.1.1.1 Componentes de la Norma

Los componentes de la norma TIA/EIA 568-A son el Cableado Horizontal, Cableado Vertical, las áreas de trabajo, los clósets de telecomunicaciones, cuartos de equipo y las entradas de servicios.

1.3.1.1.1.1 Cableado Horizontal

El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones. El cableado horizontal incluye los cables horizontales, las tomas/conectores de telecomunicaciones en el área de trabajo, la terminación mecánica y las interconexiones horizontales localizadas en el clóset de telecomunicaciones.

El cableado horizontal consiste de dos elementos básicos:

- *Cable Horizontal y Hardware de Conexión.* (también llamado "cableado horizontal") Proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el clóset de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales,
- *Rutas y Espacios Horizontales.* (también llamado "sistemas de distribución horizontal") Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el clóset de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado Horizontal. Si existiera cielo raso suspendido se recomienda la utilización de canaletas para transportar los cables horizontales, una tubería de ¾"por cada dos cables UTP, una tubería de 1" por cada cable de dos fibras ópticas, los radios mínimos de curvatura deben ser bien implementados

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. En ingles: *Work Area Outlets* (WAO),
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el clóset de telecomunicaciones,
- Paneles de empate (patch panel) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el clóset de telecomunicaciones.

Se deben hacer ciertas consideraciones a la hora de seleccionar el cableado horizontal:

1. Contiene la mayor cantidad de cables individuales en el edificio.
2. No es muy accesible; el tiempo, esfuerzo y habilidades requeridas para hacerle cambios son muy grandes.
3. Debe acomodar varias aplicaciones de usuario; para minimizar los cambios requeridos cuando las necesidades evolucionan.
4. Es necesario evitar colocar los cables de cobre muy cerca de fuentes potenciales de emisiones electromagnéticas (EMI).

Consideraciones de diseño

Los costos en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal pueden ser muy altos. Para evitar estos costos, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario. La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la relocalización de áreas de trabajo.

Al seleccionar y diseñar el cableado horizontal el diseñador debe considerar incorporar otros sistemas de información del edificio, por ejemplo: sistemas tales como televisión por cable, control ambiental, seguridad, audio, alarmas y sonido.

Topología

La norma EIA/TIA 568-A hace las siguientes recomendaciones en cuanto a la topología del cableado horizontal:

- El cableado horizontal debe seguir una topología estrella,
- Cada toma/conector de telecomunicaciones del área de trabajo debe conectarse a una interconexión en el clóset de telecomunicaciones,
- El cableado horizontal en una oficina debe terminar en un clóset de telecomunicaciones ubicado en el mismo piso que el área de trabajo servida,
- Los componentes eléctricos específicos de la aplicación (como dispositivos acopladores de impedancia) no se instalarán como parte del cableado horizontal; cuando se necesiten, estos componentes se deben poner fuera de la toma/conector de telecomunicaciones,
- El cableado horizontal no debe contener más de un punto de transición entre cable horizontal y cable plano,
- No se permiten empalmes de ningún tipo en el cableado horizontal.

Distancias

Sin importar el medio físico, la distancia horizontal máxima no debe exceder 90 m. La distancia se mide desde la terminación mecánica del medio en la interconexión horizontal en el clóset de telecomunicaciones hasta la toma/conector de telecomunicaciones en el área de trabajo. Además se recomiendan las siguientes distancias:

- Se separan 10 m para los cables del área de trabajo y los cables del clóset de telecomunicaciones (cordones de parcheo, *jumpers* y cables de equipo),
- Los cables de interconexión y los cordones de parcheo que conectan el cableado horizontal con los equipos o los cables del vertebral en las instalaciones de interconexión no deben tener más de 6 m de longitud,
- En el área de trabajo, se recomienda una distancia máxima de 3 m desde el equipo hasta la toma/conector de telecomunicaciones.

Medios reconocidos

Se reconocen tres tipos de cables para el sistema de cableado horizontal:

- Cables de par trenzado sin blindar (UTP) de 100 Ω y cuatro pares,
- Cables de par trenzado blindados (STP) de 150 Ω y dos pares,
- Cables de fibra óptica multimodo de 62.5/125 um y dos fibras.

El cable coaxial de 50 Ω aún está reconocido como un cable que se puede encontrar en instalaciones existentes; no se recomienda para las nuevas instalaciones de cableado y se espera que sea eliminado en la próxima revisión de esta norma. Se pueden emplear cables híbrido formados de más de uno de los cables anteriormente reconocidos dentro de un mismo recubrimiento, siempre que cumplan con las especificaciones.

Elección del medio

Se deben proveer un mínimo de dos tomas/conectores de telecomunicaciones para cada área de trabajo individual. Una se debe asociar con un servicio de voz y la otra con un servicio de datos. Las dos tomas/conectores de telecomunicaciones se deben configurar de la siguiente forma:

1. Una toma/conector de telecomunicaciones debe estar soportada por un cable UTP de 100 Ω y cuatro pares de categoría 3 o superior.
2. La segunda toma/conector de telecomunicaciones debe estar soportada por uno de los siguientes medios como mínimo: Cable UTP de 100Ω y cuatro pares (se recomienda categoría 5), cable STP-A de 150Ω y dos pares, Cable de fibra óptica multimodo de 62.5/125 um y dos fibras.

Consideraciones de aterrizaje

El aterrizaje debe cumplir los requerimientos y prácticas aplicables en cada caso. Además, el aterrizaje de telecomunicaciones debe estar de acuerdo a los requerimientos de la norma EIA/TIA 607.

1.3.1.1.1.2 Cableado Vertebral o Vertical

El término vertebral se emplea en lugar de vertical o *Rise"* ya que a veces este cable no corre de manera vertical (como es el caso de un campus donde el cable corre entre edificios).

La función del cableado vertebral es la de proporcionar interconexiones entre los clósets de telecomunicaciones, los cuartos de equipos y las instalaciones de entrada en un sistema de cableado estructurado de telecomunicaciones. El cableado vertebral consta de los cables vertebrales, las interconexiones principales e intermedias, las terminaciones mecánicas y los cordones de parcheo o *jumpers* empleados en la interconexión de vertebrales. El vertebral incluye también el cableado entre edificios.

Se deben hacer ciertas consideraciones a la hora de seleccionar un cableado vertebral:

1. La vida útil del sistema de cableado vertebral se planifica en varios periodos (típicamente, entre 3 y 10 años); esto es menor que la vida de todo el sistema de cableado de telecomunicaciones (típicamente, varias décadas).
2. Antes de iniciar un periodo de planificación, se debe proyectar la cantidad máxima de cable vertebral para el periodo; el crecimiento y los cambios durante ese período se deben acomodar sin necesidad de instalar cable vertebral adicional.
3. Se debe planear que la ruta y la estructura de soporte del cable vertebral de cobre evite las áreas donde existan fuentes potenciales de emisiones electromagnéticas (EMI).

Topología

La norma EIA/TIA 568-A hace las siguientes recomendaciones en cuanto a la topología del vertebral:

- El cableado vertebral deberá seguir la topología estrella convencional.

- Cada interconexión horizontal en un clóset de telecomunicaciones está cableada a una interconexión principal o a una interconexión intermedia y de ahí a una interconexión principal con la siguiente excepción: si se anticipan requerimientos para una topología de red bus o anillo, entonces se permite el cableado de conexiones directas entre los closts de telecomunicaciones.
- No debe haber más de dos niveles jerárquicos de interconexiones en el cableado vertebral (para limitar la degradación de la señal debido a los sistemas pasivos y para simplificar los movimientos, aumentos o cambios).
- Las instalaciones que tienen un gran número de edificios o que cubren una gran extensión geográfica pueden elegir subdividir la instalación completa en áreas menores dentro del alcance de la norma EIA/TIA 568-A. En este caso, se excederá el número total de niveles de interconexiones.
- Las conexiones entre dos clostes de telecomunicaciones pasarán a través de tres o menos interconexiones.
- Sólo se debe pasar por una conexión cruzada para llegar a la conexión cruzada principal.
- En ciertas instalaciones, la conexión cruzada del vertebral (conexión cruzada principal) bastará para cubrir los requerimientos de conexiones cruzadas.
- Las conexiones cruzadas del vertebral pueden estar ubicadas en los clostes de telecomunicaciones, los cuartos de equipos, o las instalaciones de entrada.
- No se permiten empalmes como parte del vertebral.

Cables reconocidos

La norma EIA/TIA 568-A reconoce cuatro medios físicos de transmisión que pueden usarse de forma individual o en combinación:

- Cable vertebral UTP de 100Ω
- Cable STP de 150 Ω
- Cable de fibra óptica multimodo de 62.5/125 um y Cable de fibra óptica monomodo

Selección del medio

Los factores que deben tomarse en cuenta cuando se hace la elección son:

- Flexibilidad respecto a los servicios soportados
- Vida útil requerida para el vertebral
- Tamaño del lugar y población de usuarios

Distancias de cableado

Las distancias máximas dependen de la aplicación. Las que proporciona la norma están basadas en aplicaciones típicas para cada medio específico. Para minimizar la distancia de cableado, la conexión cruzada principal debe estar localizada cerca del centro de un lugar. Las instalaciones que exceden los límites de distancia deben dividirse en áreas, cada una de las cuales pueda ser soportada por el vertebral dentro del alcance de la norma EIA/TIA 568-A. Las interconexiones entre las áreas individuales (que están fuera del alcance de esta norma) se pueden llevar a cabo utilizando equipos y tecnologías normalmente empleadas para aplicaciones de área amplia.

Conexión cruzada principal y punto de entrada

La distancia entre la conexión cruzada principal y el punto de entrada debe ser incluida en los cálculos de distancia total cuando se requiera.

Conexiones cruzadas

En las conexiones cruzadas principal e intermedia, la longitud de los *jumpers* y los cordones de parcheo no deben exceder los 20 m.

Cableado y equipo de telecomunicaciones

Los equipos de telecomunicaciones que se conectan directamente a las conexiones cruzadas o intermedias deben hacerlo a través de cables de 30 m o menos.

Consideraciones de aterrizaje

El aterrizaje debe cumplir los requerimientos y prácticas aplicables en cada caso. Además, el aterrizaje de telecomunicaciones debe estar de acuerdo a los requerimientos de la norma EIA/TIA 607.

1.3.1.1.1.3 Área de Trabajo

El área de trabajo se extiende de la toma/conector de telecomunicaciones o el final del sistema de cableado horizontal, hasta el equipo de la estación y está fuera del alcance de la norma EIA/TIA 568-A. El equipo de la estación puede incluir, pero no se limita a teléfonos, terminales de datos y computadoras.

Se deben hacer ciertas consideraciones cuando se diseña el cableado de las áreas de trabajo:

1. El cableado de las áreas de trabajo generalmente no es permanente y debe ser fácil de cambiar,
2. La longitud máxima del cable horizontal se ha especificado con el supuesto que el cable de parcheo empleado en el área de trabajo tiene una longitud máxima de 3 m,
3. Comúnmente se emplean cordones con conectores idénticos en ambos extremos,
4. Cuando se requieran adaptaciones especificas a una aplicación en el área de trabajo, éstas deben ser externas a la toma/conector de telecomunicaciones.

Es importante tomar en cuenta los efectos de los adaptadores y los equipos empleados en el área de trabajo antes de diseñar el cableado para evitar una degradación del rendimiento del sistema de cableado de telecomunicaciones.

Salidas de área de trabajo:

Los ductos a las salidas de área de trabajo deben prever la capacidad de manejar tres cables. Las salidas de área de trabajo deben contar con un mínimo de dos conectores. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A (recomendado) o T568B.

Algunos equipos requieren componentes adicionales (tales como *baluns* o adaptadores RS-232) en la salida del área de trabajo. Estos componentes no deben instalarse como parte del cableado horizontal, deben instalarse externos a la salida del área de trabajo. Esto garantiza la utilización del sistema de cableado estructurado para otros usos.

- Se pueden tener las siguientes adaptaciones en el área de trabajo:
- Un cable especial para adaptar el conector del equipo (host, terminal, teléfono) al conector de la salida de telecomunicaciones,
- Un adaptador en "Y" para proporcionar dos servicios en un solo cable multipar (por ejemplo: teléfono con dos extensiones),
- Un adaptador pasivo (por ejemplo: *balun*) utilizado para convertir del tipo de cable del equipo al tipo de cable del cableado horizontal,
- Un adaptador activo para conectar dispositivos que utilicen diferentes esquemas de señalización (por ejemplo: EIA 232 a EIA 422),
- Un cable con pares transpuestos.

Manejo del cable

El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm. para cables UTP categoría 5. El radio de doblado del cable no debe ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 5 el radio mínimo de doblado es de 2.5 cm.

Interferencia electromagnética

A la hora de establecer la ruta del cableado de los clósets de alambrado a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- Motores eléctricos grandes o transformadores (mínimo 1.2m),
- Cables de corriente alterna,
- Mínimo 13 cm. para cables con 2kV o menos,
- Mínimo 30 cm. para cables de 2kV a 5kV,
- Mínimo 91cm. para cables con mas de 5kV,
- Luces fluorescentes y balastros (mínimo 12cm). El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos,
- Intercomunicadores (mínimo 12cm),
- Equipo de soldadura,
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2m),
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

1.3.1.1.1.4 Clósets de Telecomunicaciones

Un clósets de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El clóset de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de clósets de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable, alarmas, seguridad, audio y otros sistemas de telecomunicaciones. No hay un

límite máximo en la cantidad de clósets de telecomunicaciones que puede haber en un edificio. Los cloets de telecomunicaciones proporcionan varias funciones diferentes a los sistemas de cableado y a menudo son tratados como subsistemas diferentes dentro de la jerarquía de estos.

Diseño y Características

Si se realiza integralmente el cableado de telecomunicaciones, debe brindar servicio de transmisión de datos y telefonía, existen por lo menos dos alternativas para la interconexión de los montantes telefonía con el cableado a los puestos de trabajo:

1. Utilizar regletas (bloques de conexión) que reciben los cables del montante por un extremo y de los puestos de trabajo por el otro, permitiendo la realización de las cruzadas de interconexión.
2. Utilizar paneles de empate para terminar las montantes telefónicas y el cableado horizontal que se destinará a telefonía, implementando los cordones de empate. Esta alternativa, de costo algo mayor, es la más adecuada tecnológicamente y la que responde más adecuadamente al concepto de cableado estructurado, ya que permite la máxima sencillez convertir datos a telefonía y viceversa.

El diseño de un clóset de Telecomunicaciones depende de: El tamaño del edificio, el espacio de piso a servir, las necesidades de los ocupantes, los servicios de telecomunicaciones a utilizarse.

Debe de haber al menos un cuarto de Telecomunicaciones por edificio, mínimo uno por piso, no hay máximo. La altura mínima recomendada del cielo raso es de 2.6 metros. El número y tamaño de los ductos utilizados para accesar el clóset de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo, sin embargo se recomienda por lo menos tres ductos de 100mm (4”) para la distribución del cable del Backbone. Los ductos de entrada deben de contar con elementos de retardo de propagación de incendio *"firestops"*. Entre clósets de telecomunicaciones de un mismo piso debe haber mínimo un tubo conduit de 75mm. La(s) puerta(s) de acceso debe(n) ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto. La puerta debe ser removible y abrir hacia afuera (o lado a lado). La puerta debe abrir al ras del piso y no debe tener postes centrales. Se debe el evitar polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática. En clósets que no tienen equipo electrónico la temperatura debe mantenerse continuamente (24 horas al día, 365 días al año) entre 10ºC y 35ºC. La humedad relativa debe mantenerse menor a 85%. Debe de haber un cambio de aire por hora. En clósets que tienen equipo electrónico la temperatura debe mantenerse continuamente (24 horas al día, 365 días al año) entre 18ºC y 24ºC. La humedad relativa debe mantenerse entre 30% y 55%. Debe de haber un cambio de aire por hora. Se debe evitar el uso de cielos falsos en los clósets de telecomunicaciones. Los clósets de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el clóset de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso. De haber regaderas contra incendio, se debe instalar una canoa para drenar un goteo potencial de las regaderas. Los pisos de los CT deben soportar una carga de 2.4kPa. Los clósets deben de estar bien iluminados, se recomienda que la iluminación debe de estar a un mínimo de 2.6m del piso terminado, las paredes y el techo deben de estar pintadas de preferencia de colores claros para obtener

una mejor iluminación, también se recomienda tener luces de emergencia por si al foco se daña. Se debe proporcionar un mínimo equivalente a 540 lux medido a un metro del piso terminado. Con el propósito de mantener la distancia horizontal de cable promedio en 46m o menos (con un máximo de 90m), se recomienda localizar el clóset de telecomunicaciones lo más cerca posible del centro del área a servir. Debe haber tomacorrientes suficientes para alimentar los dispositivos a instalarse en los andenes. La norma establece que debe haber un mínimo de dos tomacorrientes dobles de 110V CA dedicados de tres hilos. Deben ser circuitos separados de 15 a 20A. Estos dos tomacorrientes podrían estar dispuestos a 1.8m de distancia uno de otro. Considerar alimentación eléctrica de emergencia con activación automática. En muchos casos es deseable instalar un panel de control eléctrico dedicado al clóset de telecomunicaciones. La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los andenes. Separado de estas tomas deben haber tomacorrientes dobles para herramientas, equipo de prueba, etc. Estos tomacorrientes deben estar a 15cm del nivel del piso y dispuestos en intervalos de 1.8m alrededor del perímetro de las paredes. El clóset de telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable de mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA-607. Se debe mantener el clóset de telecomunicaciones con llave en todo momento. Se debe asignar llaves a personal que esté en el edificio durante las horas de operación. Se debe mantener el clóset de telecomunicaciones limpio y ordenado. Al menos dos de las paredes del cuarto deben tener láminas de plywood A-C de 20mm de 2.4m de alto. Las paredes deben ser suficientemente rígidas para soportar equipo. Las paredes deben ser pintadas con pintura resistente al fuego, lavable, mate y de color claro.

Debe haber al menos un clóset de telecomunicaciones o cuarto de equipo por piso y por áreas que no excedan los 1000m^2. Instalaciones pequeñas podrán utilizar un solo clóset de telecomunicaciones si la distancia máxima de 90m no se excede.

Área a Servir Edificio Normal	**Dimensiones Mínimas del Cuarto de Alambrado**
500m^2 o menos	3.0m x 2.2m
mayor a 500m^2, menor a 800m^2	3.0m x 2.8m
mayor a 800m^2, menor a 1000m^2	3.0m x 3.4m
Área a Servir Edificio Pequeño	Utilizar para el Alambrado
100m^2 o menos	Montante de pared o gabinete encerrado
Mayor a 500m^2 , menor a 800m^2	Cuarto de 1.3m x 1.3m o Clóset angosto de 0.6m x 2.6m
* Algunos equipos requieren un fondo de al menos 0.75m	

Tabla 22. Dimensiones del cuarto de alambrado en relación con el área de servicio del edificio.

Disposición de equipos

- Los andenes (racks) deben de contar con al menos 82cm de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82cm se debe medir a partir de la superficie más salida del andén,
- De acuerdo al NEC, NFPA-70 Artículo 110-16, debe haber un mínimo de 1m de espacio libre para trabajar de equipo con partes expuestas sin aislamiento,

- Todos los andenes y gabinetes deben cumplir con las especificaciones de ANSI/EIA-310,
- La tornillería debe ser métrica M6,
- Se recomienda dejar un espacio libre de 30cm en las esquinas.

Funciones

Un clóset de telecomunicaciones tiene las siguientes funciones:

1. La función principal de un clóset de telecomunicaciones es la terminación del cableado horizontal en hardware de conexión compatible con el tipo de cable empleado,
2. El vertebral también se termina en un clóset de telecomunicaciones en hardware de conexión compatible con el tipo de cable empleado,
3. La conexión cruzada de las terminaciones de cables horizontales y vertebral mediante *jumpers* o cordones de empate permite una conectividad flexible cuando se extienden varios servicios a las tomas/conectores de telecomunicaciones de las áreas de trabajo. El hardware de conexión, los *jumpers* y los cordones de empate empleados para este propósito son llamados colectivamente conexión cruzada horizontal,
4. Un clóset de telecomunicaciones puede contener también las conexiones cruzadas intermedias o principales para diferentes porciones del sistema de cableado vertebral,
5. En ocasiones, las conexiones cruzadas de vertebral a vertebral en el cuarto de telecomunicaciones se emplean para unir diferentes clósets de telecomunicaciones en una configuración anillo, bus, o árbol,
6. Un clóset de telecomunicaciones proporciona también un medio controlado para colocar los equipos de telecomunicaciones, hardware de conexión o cajas de uniones que sirven a una porción del edificio,
7. En ocasiones, el punto de demarcación y los aparatos de protección asociados pueden estar ubicados en el clóset de telecomunicaciones.

Conexiones cruzadas e interconexiones

La norma EIA/TIA 568-A hace las siguientes recomendaciones:

- Los cableados horizontal y vertebral deben estar terminados en hardware de conexión que cumpla los requerimientos de la norma EIA/TIA 568-A,
- Todas las conexiones entre los cables horizontal y vertebral deben ser conexiones cruzadas,
- Los cables de equipo que consolidan varios puertos en un solo conector deben terminarse en hardware de conexión dedicado,
- Los cables de equipo que extienden un solo puerto deben ser terminados permanentemente o interconectados directamente a las terminaciones del horizontal o del vertebral,
- Las interconexiones directas reducen el número de conexiones requeridas para configurar un enlace y esto puede reducir la flexibilidad.

1.3.1.1.1.4.1 Clasificación de los Clósets de Telecomunicaciones

Durante años la Industria Telefónica ha usado los términos de *Intermediate Distribution Trama* (IDF) y *Main Distribution Trama* (MDF) para referirse a diversos elementos en el

cableado estructurado. Como la popularidad del cableado estructurado ha crecido a la par de las comunicaciones de datos, esta terminología es muy común en nuestros días.

1.3.1.1.1.4.1.1 IDF

Los cuartos IDF son usados para conectar los equipos terminales, como los hosts y terminales, a la red. Esta conexión horizontal conecta las rosetas situadas en la pared y típicamente consiste de cable UTP (Unshielded Twisted-Pair) que forma una topología física de estrella hacia el IDF. Como se muestra en la Figura 36, cada piso del edificio generalmente contiene uno o más switches IDF. Cada host se conecta hacia el cuarto de instalación IDF más cercano. Todos los IDFs en el edifico generalmente se conectan a un par de equipos MDF, a menudo localizados en la base del edificio o en la planta baja.

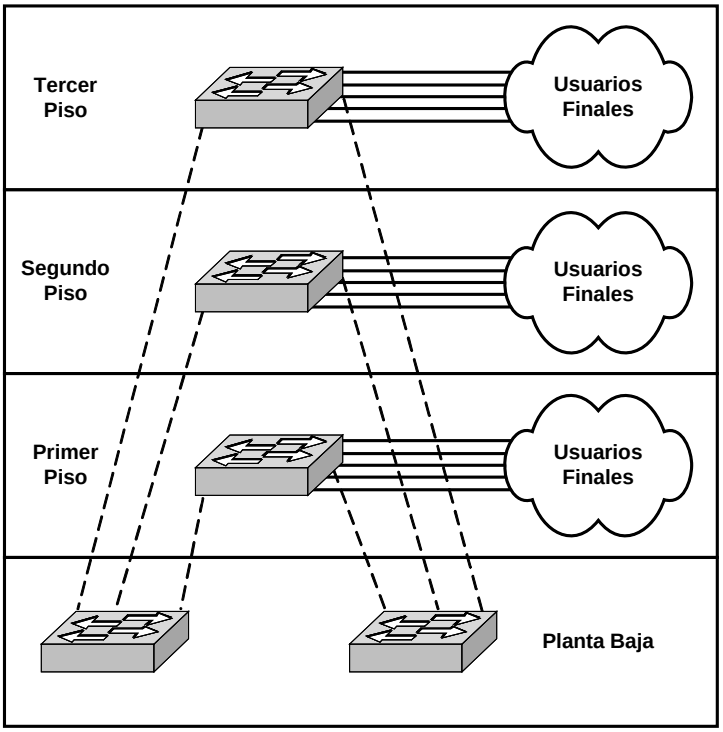


Figura 36. Cuartos IDF Múltiples.

Los IDF poseen varios requerimientos específicos de acuerdo al desempeño que deben tener, a continuación se mencionan:

- *Densidad por Puerto:* Debido a que un gran número de hosts necesitan conectarse a cada IDF, una alta densidad de puerto es requisito indispensable,
- *Costo por Puerto:* Dada la alta densidad en el puerto que se encuentra en un IDF típico, el costo por puerto debe ser razonable,
- *Redundancia:* Porque varias decenas de equipos son conectados a menudo hacia los equipos de comunicaciones en los IDFs, una simple falla en el IDF puede crear una interrupción considerable en la red,
- *Confiabilidad:* Debido a que cada equipo de comunicación en el IDF posee el único enlace hacia el resto de la red para cada host,

➢*Facilidad en Administración:* El gran número de conexiones requiere que la administración por puerto sea la mínima posible,

Debido a que existen demasiados usuarios finales conectados, la redundancia y la confiabilidad son un aspecto crítico en el papel de los IDFs. Como resultado, los IDF no solo deberían usar hardware redundante, como lo son los supervisores duales o las fuentes de poder, si no también enlaces múltiples hacia los equipos de comunicación situados en los MDF. Las fallas de esto equipos de comunicación también son críticas.

La confiabilidad en los IDFs nos trae un punto importante en lo que respecta a las conexiones de los hosts. Fuera de los ambientes limitados como los pisos financieros, generalmente no afecta en el costo tener hosts conectadas a más de un equipo de comunicación en los IDFs. Por consiguiente, el cableado horizontal es un simple punto de falla para muchas redes. Sin embargo, considerando que estas fallas solo afectan a los usuarios finales. Estas fallas son de menor magnitud comparadas con la perdida completa de un switch. Para hosts importantes como lo son los servidores, las tarjetas de interface de red duales (NICs) pueden ser utilizadas con enlaces múltiples para proveer redundancia hacia los clósets de switches.

El equipo tradicional que es usado en los IDF, es el concentrador. Debido a que los concentradores son equipos realmente simples, el costo por puerto es muy bajo y atractivo. Sin embargo, gracias a su naturaleza compartida obviamente provee menos ancho de banda disponible para los usuarios finales. Por otro lado, los enrutadores y switches de capa 3 pueden proveer inteligencia ala hora de compartir el ancho de banda, pero generalmente estos equipos son muy caros y tienen una densidad por puerto limitada.

Si se quiere hacer un balance entre costo, ancho de banda disponible y densidad por puerto, muchas de las redes actualmente diseñadas utilizan switches de capa 2 en los IDF. Esta es una manera de hacer efectivo el costo para proveer 500 o más hosts con acceso de alta velocidad hacia el Backbone del campus.

1.3.1.1.1.4.1.2 MDF

Los equipos instalados en los IDFs colapsan hacia uno o más equipos de comunicación instalados en los MDFs. Cada IDF a menudo esta conectado a dos diferentes equipos en el MDF para proveer una adecuada redundancia. Algunas organizaciones colocan ambos equipos MDF en el mismo clóset y confían en el enrutamiento para proveer redundancia. Otras organizaciones prefieren colocar los equipos de comunicación en MDFs separados uno del otro. La relación entre los edificios y los MDFs no es una regla que se tenga que seguir al pie de la letra, los edificios grandes posiblemente poseen más de dos switches instalados en el MDF, mientras un par de equipos redundantes instalados en el MDF pueden trabajar perfectamente con varios edificios más pequeños en tamaño.

La Figura 37 muestra tres edificios con sus respectivos cuartos MDF. Para cumplir con la redundancia requerida, cada edificio generalmente aloja dos equipos de comunicación instalados en cada MDF. Los equipos instalados en el MDF también pueden ser para interconectar a los tres edificios.

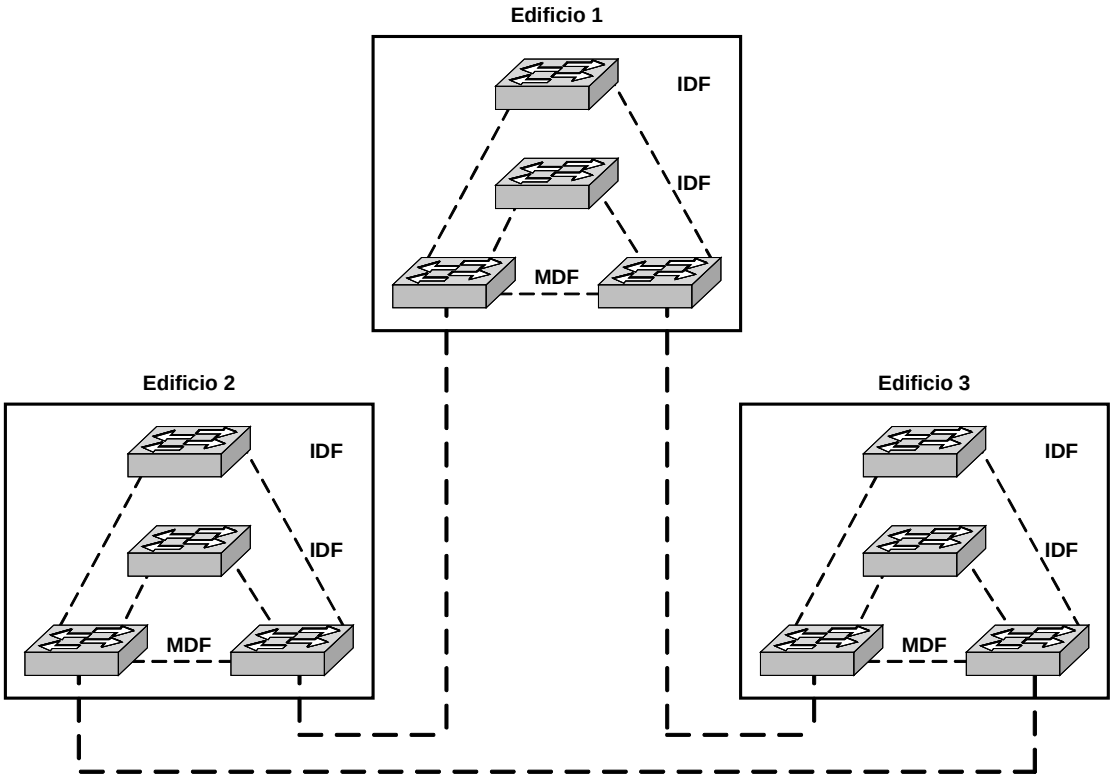


Figura 37. Cuartos MDF.

Los cuartos MDF tienen otros requerimientos con respecto a los cuartos IDF:

- Rendimiento en procesamiento,
- Alta Disponibilidad,
- Capacidades de Enrutamiento.

Dado que los MDFs actúan como un punto de concentración para el tráfico proveniente de los IDFs, los equipos instalados en el MDF deben ser capaces de procesar altos niveles de tráfico. En el caso de los switches de capa 2, el ancho de banda es fácilmente disponible y barato. Sin embargo, muchas de las estrategias para lograr diseños robustos y escalables requieren de enrutamiento en los MDFs. Lograr este nivel de desempeño de capa 3 requiere una cuidadosa planeación.

La alta disponibilidad es un requerimiento de suma importancia para los equipos instalados en los cuartos MDF. Aunque la falla de algún switch instalado en un IDF o MDF puede afectar potencialmente a muchos usuarios finales, hay una diferencia sustancial entre estas dos situaciones. Como se vio anteriormente, una falla en un IDF puede afectar a una gran cantidad de usuarios finales, en cambio, una falla en un MDF raramente resulta en una pérdida completa de conectividad, esto debido a que los equipos instalados en los MDFs siempre están desplegados en pares. Sin embargo, esto no significa que las fallas en los MDFs son inconsecuentes. Por el contrario, las fallas en los MDFs afectan a menudo a miles de usuarios, muchos más que con una falla en un IDF.

Además, otras características de enrutamiento pueden ser importantes en las situaciones de los MDFs. Por ejemplo, que protocolos de capa 3, que el enrutador pueda manejar, son importantes (IP. IPX. AppleTalk y así sucesivamente). Los protocolos de enrutamiento (OSPF, RIP, EIGRP, IS-IS, etc) soportados puede ser otro factor importante. Soporte de características como lo son DHCP y HSRP también pueden provocar problemas.

Los tres tipos de equipos pueden ser utilizados en un MDF son:

- Switches de capa 2
- Enrutadores
- Switches de capa 3

El primero es el más simple. Un switch de capa 2 tiene un costo moderado y un alto rendimiento en procesamiento, por lo que estos equipos son una buena opción.

Sin embargo, como ya sabemos hay buenas razones para utilizar procesamiento de capa 3 en los MDFs. Esto conduce a muchos diseños de red a utilizar la tercera opción, un switch de capa 3 que esta funcionando como un enrutador basado en hardware.

1.3.1.1.1.5 Cuartos de Equipos

Los cuartos de equipos son considerados de manera diferente que los clósets de telecomunicaciones debido a la naturaleza o complejidad de los equipos que ellos contienen. Todas las funciones de los clósets de telecomunicaciones deben ser proveídas por los cuartos de equipos.

El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Varias o todas las funciones de un clósets de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los clósets de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un clóset de telecomunicaciones o un cuarto de equipo. Los requerimientos del cuarto de equipo se especifican en las normas ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

Funciones

Un cuarto de equipos debe proveer las siguientes funciones:

1. Un ambiente controlado para los contenedores de los equipos de telecomunicaciones, el hardware de conexión, las cajas de uniones, las instalaciones de aterrizaje y sujeción y los aparatos de protección, dónde se necesiten,
2. Desde una perspectiva del cableado, o las conexión cruzada principal o la intermedia usada en la jerarquía del cableado vertebral,
3. Puede contener las terminaciones de los equipos (y puede contener las terminaciones horizontales para una porción del edificio),
4. A menudo contiene las terminaciones de la red troncal/auxiliar bajo el control del administrador del cableado local.

1.3.1.1.1.6 Cuarto de Entrada de Servicios

El cuarto de entrada de servicios consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto ó espacio de entrada. El cuarto de entrada puede incorporar el Backbone que conecta a otros edificios en situaciones de campo los requerimientos de los cuartos de entrada se especifican en las normas ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569. El cuarto de entrada de servicios consta de los cables, hardware de conexión, dispositivos de protección, hardware de transición, y otro equipo necesario para conectar las instalaciones de los servicios externos con el cableado local. El punto de demarcación entre las portadoras reguladas o los proveedores de servicio y el cableado local del cliente debe ser parte de la instalación de entrada.

Funciones

Una instalación de entrada debe proporcionar:

1. Un punto de demarcación de red entre los proveedores de servicio y el cableado local del cliente,
2. Ubicación de la protección eléctrica gobernada por los códigos eléctricos aplicables,
3. Una transición entre el cableado empleado en planta externa y el cableado aprobado para distribución en interiores.

Esto implica a menudo una transición a un cable con especificaciones contra la propagación de fuego.

1.3.1.1.2 TSB 75: Prácticas Adicionales de Cableado para Oficinas Abiertas

Cuando se instala una línea de gran distancia, y luego de ello se hacen cambios en los muebles modulares, se tiene que desechar todo el cable instalado, esto es muy costoso, por lo que esta norma permite una manera de administrar un sistema de cable centralizado, a la vez que permite hacer cambios o remodelaciones fáciles en oficinas abiertas, especifica prácticas adicionales para este tipo de entornos y permite cambios en el cableado cuando los muebles modulares de oficinas son reorganizados. Solamente se puede utilizar este esquema en sistema de muebles modulares y esta prohibido en oficinas con paredes falsas o ladrillos.

Se tiene dos configuraciones permitidas:

1. Ensamble de salidas de Telecomunicaciones Multiusuarios (MUTO, Multiuser Telecommunications Outlet Assambly),
2. Punto de Consolidación.

Para la configuración MUTO, los cables horizontales terminan en un lugar común y los cordones de empate se enrutan directamente del MUTO al área de trabajo. Esta solución se recomienda para aplicaciones donde se anticipan movimientos frecuentes, cada MUTO debe dar servicio a un máximo de 6 áreas de trabajo o 12 salidas, debe ser fácilmente

accesible y no estar localizado en un piso o techo falso, debe quedar instalado de forma permanente.

La longitud máxima de los cordones de empate de host no deberá ser mayor a 20m, aunque la distancia al MUTO sea menor a 70m en lo que respecta al cableado horizontal. La distancia máxima no debe rebasar nunca los 100m para cableado de cobre. Para el cableado con fibra se permite cualquier combinación de longitud en cables horizontales, cables de área de trabajo, cordones de empate y cables de equipo, la distancia máxima es de 100m. En la Tabla 23 se muestran las longitudes de cable.

Longitud de Cable Horizontal	Longitud Máxima para Cable de Área de Trabajo	Longitud Máxima para cables área de trabajo, patch cords y cable de equipo
m	m	m
90	3	10
85	7	14
80	11	18
75	15	22
70	20	27

Tabla 23. Longitudes para cables para conexiones en configuración MUTO.

En lo que respecta a la configuración de Punto de Consolidación se puede mencionar que se trata de un punto de interconexión en el cableado horizontal, es recomendable cuando se anticipa una gran cantidad de cambios, nunca se debe usar como conexión cruzada, no se permite más de uno entre cada corrida, se recomienda instalar el Punto de Consolidación a una distancia de 15m del clóset de telecomunicaciones. Cada punto de Consolidación debe dar servicio a un máximo de 6 áreas de trabajo o 12 salidas, debe quedar completamente accesible e instalado permanentemente y la distancia del enlace se limita a los 90m (más 10m de patch cord).

1.3.1.1.3 TSB 72: Cableado de fibra Óptica Centralizado

Esta norma fue publicada en octubre de 1995 y específica las guías y requerimientos de los equipos de conexión para implantar cableados de fibra óptica centralizados, cumple con la norma TIA/EIA-568-A.

Los requerimientos necesarios para implementar esta norma son los siguientes: el cableado centralizado se localizará en el mismo edificio que el área de trabajo, todos los cambios y movimientos se realizarán en la conexión cruzada centralizada, los cambios en los enlaces horizontales se realizarán en el clóset de telecomunicaciones y no se debe dar servicio a otro edificio.

Existen alternativas de conexiones cruzadas:

Registros de Cables: Un cable continuo que parte desde la conexión cruzada centralizada, pasa por el clóset de telecomunicaciones hasta el área de trabajo, la longitud

entre la conexión cruzada y el área de trabajo será de 300 m máximo y los requerimientos de los cables tal como los señala la norma TIA/EIA-568-A.

*Interconexión y Empalme**:*** Esta alternativa incrementa la flexibilidad y facilidad para migrar hacia una conexión cruzada, la longitud entre la conexión cruzada y el área de trabajo deberá ser de 300 m máximo.

El cableado centralizado deberá permitir migrar a una conexión cruzada, así como agregar o remover cables de fibra óptica: verticales y horizontales. Debemos asegurar la correcta polaridad de la fibra, proveer control del radio de curvatura y administrar la reserva de cable.

El equipo de Interconexión debe cumplir con la norma TIA/EIA-568-A y debe proveer una protección adecuada para los conectores.

1.3.1.2 TIA/EIA 569-A: Norma para Rutas y Espacios en Edificios Comerciales

Esta norma reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

1. Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son más la regla que la excepción.
2. La norma reconoce, de manera positiva, que el cambio ocurre.
3. Los sistemas de telecomunicaciones y de medios son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones cambian dramáticamente. Esta norma reconoce este hecho siendo tan independiente como sea posible de proveedores de equipo.

Esta norma reconoce un precepto de fundamental importancia: De manera que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

Esta norma se refiere al diseño especifico sobre la dirección y construcción, los detalles del diseño para el camino y espacios para el cableado de telecomunicaciones y equipos dentro de edificios comerciales.

- *EF.* Es el espacio que provee un punto de presencia y la terminación del cableado en el edificio de la parte exterior. El EF puede también distribuir cableado horizontal para el área de trabajo como se muestra una función como un TC.
- TC. El TC puede alojar también equipos de telecomunicaciones y puede funcionar como un cuarto de equipo ER.
- *WA.* El WA es el espacio donde ocupan recíprocamente equipos de telecomunicaciones.

El propósito de esta norma es llevar las prácticas de diseño y construcción de los componentes de la red que darán soporte a los medios de transmisión (ductos) y al equipo de telecomunicaciones (clósets y espacios).

Esta norma es aplicable a aspectos de telecomunicaciones en el diseño y construcción de edificios comerciales y no incluye aspectos de seguridad en el diseño del edificio. Abarca los siguientes aspectos:

1.3.1.2.1 Rutas de Cableado Horizontal

Son las facilidades para la instalación del cable desde el clóset de telecomunicaciones hasta el área de trabajo, estas rutas incluyen: ducto bajo el piso, piso falso, tubo conduit, charolas para el cable, rutas de techo falso y rutas perimetrales.

- *Ducto bajo el piso:* es la distribución de ductos empotrados en el concreto, forma rectangular, en varios tamaños con o sin inserciones predeterminadas,
- *Piso falso:* Son paneles modulares de piso apoyados por pedestales,
- *Tubo Conduit:* Tubería metálica eléctrica, rígida o de PVC. Se deberá usar en rutas horizontales solamente cuando las localizaciones de salidas son permanentes, la densidad del cableado es baja y no se requiere flexibilidad. Cualquier corrida de Conduit no deberá servir a más de 3 salidas, ninguna sección deberá ser mayor de 30 m o contener más de 2 ángulos de 90º sin un registro,
- *Escalerilla para cable:* Estructuras rígidas para el soporte de cables de telecomunicaciones con una altura máxima de acceso de 0.3 m por encima de ella,
- *Rutas de techo falso:* Las láminas del cielo raso deben ser móviles y estar colocadas a una altura máxima de 3.6 m sobre el piso, las áreas de techo falso inaccesible no deben ser utilizadas como rutas de distribución,
- *Tipos de rutas perimetrales:* Ductos para superficies, empotrados, tipo moldura y multicanal.

1.3.1.2.2 Rutas de Cableado Vertical

Son las rutas dentro y entre edificios, físicamente pueden ser verticales u horizontales.

Dentro del edificio son de tubo conduit, acopladores y ranuras y conecta la entrada de servicios a los clósets de telecomunicaciones, debe tenerse un tubo conduit de 4'' por cada 5000 m^2 de espacio utilizable más dos tubos conduit adicionales para crecimiento o respaldo por fallas, equipados con protección contra fuego.

Las rutas entre edificios interconectan plantas o campus, pueden ser subterráneas, directamente enterradas, aéreas y de túnel. Además, estas rutas deben ser resistentes a la corrosión, las rutas metálicas deben estar aterrizadas, la separación de las instalaciones eléctricas debe ser de acuerdo a los códigos aplicables.

1.3.1.3 TIA/EIA 606: Norma de Administración para la Infraestructura de Telecomunicaciones en Edificios Comerciales

El propósito de esta norma es proporcionar un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. La norma establece

guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

La Tabla 24 muestra el código de color en los cables, para proveer un esquema de información sobre la administración del camino para el cableado de telecomunicación, espacios y medios independientes. Marcando con un código de color y grabando en estos los datos para la administración de los cables de telecomunicaciones para su debida identificación.

Color	Tipo
Naranja	Terminación central de oficina
Verde	Conexión de red / circuito auxiliar
Púrpura	Conexión mayor / equipo de datos
Blanco	Terminación de cable MC a IC
Gris	Terminación de cable IC A MC
Azul	Terminación de cable horizontal
Café	Terminación de cable del campus
Amarillo	Mantenimiento auxiliar, alarmas y seguridad
Rojo	Sistema Telefónico

Tabla 24. Código de colores y elemento representativo

Esta norma provee un esquema uniforme de administración de las siguientes áreas: terminaciones, medios, rutas, espacios y puestas a tierra. Este esquema es independiente de las aplicaciones y la información puede ser presentada mediante etiquetas, registros, reportes, planos y órdenes de trabajo.

1.3.1.3.1 Etiquetas

El etiquetado puede realizarse mediante etiquetas individuales fijamente sujetadas a los elementos o marcando directamente cada elemento.

- *Etiquetado de las rutas:* Las rutas deben ser etiquetadas en todos los puntos de terminación, en las localizaciones intermedias no es obligatorio pero si muy deseable,
- *Etiquetado de los espacios:* Todos los espacios deben ser rotulados, se recomienda que las etiquetas se fijen en la entrada de cada espacio,
- *Etiquetas de terminación:* Los accesorios de terminación (como los paneles) deben ser etiquetados con un identificador único, cada posición de terminación debe también ser marcada con un identificador único.

Los cables verticales y horizontales deben ser etiquetados en cada extremo, la rotulación en localizaciones intermedias no es obligatoria, pero es útil. Es altamente recomendable que se usen etiquetas adhesivas en lugar de marcar directamente sobre el cable.

Existen tres tipos de etiquetas:

1. *Adhesivas*. Existen pre-impresas, matriz de puntos o para impresoras láser, deben escogerse materiales para el ambiente especifico. Para el cable se tienen que utilizar etiquetas auto-laminables para envolverlo.

2. *De inserción*. Este tipo de etiquetas deben estar sujetas firmemente bajo condiciones normales de operaciones.

3. *Otras etiquetas*. Pueden ser de amarre o de código de barras, etc.

1.3.1.3.2 Registros

Deben contener la recolección de la información relacionada con un elemento específico, esto incluye identificadores y conexiones.

- *Identificadores:* se asignan a un elemento para conectarlo a su registro correspondiente. En la Tabla 25 se muestras tipos de identificadores.

Elemento	Identificador
Cable	C xxx
Clóset de Telecomunicaciones	TC xxx
Área de Trabajo	WA xxx
Tubería Conduit	Cd xxx

Tabla 25. Ejemplos de identificadores

Los identificadores pueden ser codificados o no codificados (J0003, J3A-C35-09).

- *Conexiones:* La conexión lógica entre los identificadores y los registros necesita de enlaces, que son los puntos en donde la información se localiza y son referencia cruzada para otra información relacionada.

Para registrar un cable conceptualmente necesitamos la información siguiente:

Identificador del cable: A0001 y tipo de cable: 4-pr UTP, Cat 5.

Los enlaces requeridos son:

Registro de terminación: J3A-C35-09, Registro de la ruta: Cd 15 y registro del equipo: PC238.

Información adicional: longitud del cable 68 m.

1.3.1.3.3 Reportes

Presentan la información seleccionada de varios registros, pueden ser generados a partir de un juego de registros o de varios registros seleccionados, por ejemplo para reportar conceptualmente un cable se tiene lo siguiente:

Cable ID: C00023
Ruta: CD35
Posición de terminación 1: A0038
Posición de terminación 2: 3A-C17-001

Espacio 1: D306
Espacio 2: 3ª
Tipo: 4prUTPCat5
Longitud: 78m

- *Reportes de rutas:* Listar todas las rutas, sus tipos, porcentaje de capacidad, carga y contenido,
- *Reportes de espacio:* Listar todos lo espacios, sus tipos y localización,
- *Reportes de cables:* Se recomienda listar todos los cables, su tipo y posiciones de terminación,
- *Reporte de conexiones cruzadas:* listar cada espacio y las conexiones cruzadas que tiene.

1.3.1.3.4 Planos

Se usan para ilustrar las diferentes etapas de planeación e instalación de cableado; conceptual, instalación y registro. Muestran la localización y tamaño de las rutas y espacios, debe aparecer el identificador de cada ruta y espacio representado. Además los planos indican la ruta de todos los cables, el plano del nivel debe mostrar las localizaciones de todas las salidas para telecomunicaciones así como la localización de todos los empalmes.

1.3.1.3.5 Ordenes de Trabajo

Documentan las operaciones necesarias para implementar acciones o cambios, deben listar tanto al personal responsable de las operaciones físicas, como a los que sean responsables de actualizar la documentación.

1.3.1.4 TIA/EIA 607: Norma de requerimientos para Uniones y Puestas a Tierra para Telecomunicaciones en Edificios Comerciales

El objetivo de esta norma es permitir la planeación, diseño e instalación de sistemas de tierra para telecomunicaciones en un edificio con o sin conocimiento previo de sistemas de telecomunicaciones subsecuentemente instalados.

Especifica la conexión a los sistemas de tierra del edificio y su soporte a equipos y sistemas de telecomunicaciones. Esta infraestructura de unión y puesta a tierra de telecomunicaciones en conjunción con sistemas de tierra eléctricos, protección antirayos, y sistema de agua forman el sistema de tierra del edificio.

Los elementos que componen esta estructura son:

*Conductor de unión para telecomunicaciones***.** Es el cable principal de Puesta a Tierra tiene la función de unir la Barra principal de puesta a Tierra para telecomunicaciones con la tierra del servicio eléctrico del edificio. El conductor de unión para Telecomunicaciones deberá ser como mínimo del mismo calibre que el TBB.

Barra principal de puesta a tierra para telecomunicaciones (TMBG-Telecommunications Main Grounding Busbar). La TMGB funciona como la extensión del electrodo de tierra del edificio para la infraestructura de telecomunicaciones, además de servir como el punto principal de unión para las TBB's y equipo, típicamente tiene que haber una TMGB por edificio. Las extensiones de la TMGB deberán ser la Barras de Puesta a Tierra para Telecom (TGB's).

En cuanto a instalación la TMGB debe ser accesible al personal de telecomunicaciones, el lugar ideal para instalarla es donde está localizada la entrada de servicios ya que la TMGB debe dar servicio al equipo de telecomunicaciones localizado en el mismo clóset o espacio, tiene que estar tan cerca como sea posible (y práctico) del panel principal de telecomunicaciones y conectarse a él por medio de su cubierta metálica.

La TMGB es una barra de cobre pre-perforada para los conectores a utilizar. Es deseable que esté platinada para reducir la resistencia de contacto, si no lo está, deberá limpiarse antes de colocar los conductores. Deberá tener una dimensión mínima de 6 mm de grueso por 100 mm de ancho y longitud variable. Esta barra deberá estar separada y aislada de su soporte, se recomiendan 5 cm. Deberá colocarse tratando de tener la ruta más recta y estar lo más cerca posible de los protectores primarios de telecomunicaciones, el conductor que los une tiene como finalidad el guiar los rayos y corrientes de falla AC hacia los protectores primarios de telecomunicaciones. Debe mantenerse un mínimo de 30 cm de separación entre este conductor y cualquier cable de potencia, de datos y/o control aún cuando se encuentre dentro de conduit metálico.

Los conectores para el conductor de unión de telecomunicaciones a la TMGB deben ser de compresión exotérmica o equivalente. La conexión de conductores para unir equipo de telecomunicaciones a la TMGB puede usar conectores de compresión por tornillo de una perforación, aunque se prefieren conectores de compresión de dos perforaciones

Unión Vertical para telecomunicaciones (TBB-Telecommunications Bonding Backbone). Es un conductor continuo que tiene como función principal reducir e igualar las diferencias de potencial entre los sistemas de telecomunicaciones unidos a ella. Interconecta todas las TGB's con la TMGB. Una TBB no está destinada a ser el único conductor que provee camino para la corriente de falla a tierra, ya deberá existir uno en el edificio para la distribución eléctrica.

Se usa un conductor metálico de comprensión no reversible, o se fusiona con soldadura exotérmica (cable de cobre aislado: AWG 6 - AWG 3). Deberá ser consistente con el sistema vertical y permitir múltiples TBB's determinados por el tamaño del edificio, además el sistema de agua NO puede ser usado como TBB.

Cuando dos o más TBB's verticales se usen en un mismo edificio de varios pisos, las TBB's deberán unirse con un Conductor de Unión Vertical de Interconexión para Telecom. (TBBIBC) en el último piso y por lo menos cada tres pisos en el medio. Durante la instalación deberán evitarse empalmes y si se usan, estos deben estar en un espacio de telecomunicaciones usando conectores de comprensión irreversible, soldadura exotérmica o equivalente.

Barra de puesta tierra pata telecomunicaciones (TGB-Telecommunications Grounding Busbar). Esta barra es el punto de conexión común para los sistemas de

telecomunicaciones y equipo usados en el clóset de telecomunicaciones o cuarto de equipo.

LA TGB tiene las siguientes dimensiones mínimas: 6mm de grueso por 50 mm de alto y una longitud variable. Se desea que esté platinada para reducir la resistencia al contacto, si no lo está, limpiarla perfectamente antes de colocar los conductores. Al igual que la TMGB, la TGB tiene que estar separada y aislada de su soporte, se recomiendan 5cm.

El conductor de unión entre la TBB y la TGB debe ser continuo y enrutado por el camino más corto posible, además tiene que estar tan cerca como sea posible y práctico del panel de telecomunicaciones, al cuál tiene que conectarse en su cubierta metálica. Las conexiones entre las TBB's y la TGB usará conectores de compresión de dos perforaciones. Cada TGB deberá unirse a la estructura del edificio por medio de un conector AWG 6, siempre y cuando la estructura se encuentre puesta a tierra en forma efectiva.

Cada cuarto de equipo y clóset de telecomunicaciones debe contener un TGB para proveer de máxima flexibilidad y accesibilidad para poner a tierra los sistemas de telecomunicaciones.

Conductor de unión vertical de interconexión para telecomunicaciones (TBBIBC-Telecommunications Bonding backbone Interconnecting Bonding Conductor). Es el cierre, balancea la diferencia de potencial.

Par unir todos estos componentes se usarán conductores de cobre aislado, el tamaño mínimo del conductor será calibre AWG 6. Los conductores de unión NO deberán colocarse en tubos conduit metálicos. Si es necesario hacerlo en una longitud que exceda 1m, los conductores de unión deberán unirse al tubo conduit en cada extremo con un cable calibre AWG 6 como mínimo. Cada conductor de unión para telecomunicaciones deberá estar etiquetado, estas etiquetas deben estar lo más cercanas al punto de terminación y no deberán ser metálicas.

1.3.2 Tipos de Cable

La transmisión de datos binarios en el cable se hace aplicando voltaje en un extremo y recibiéndolo en otro extremo. Algunos de estos cables se pueden usar como medio de transmisión: Cable Recto, Cable Coaxial, Cable UTP, Fibra óptica, Cable STP, sin embargo para la instalación de un sistema de cableado estructurado los más recomendados son: UTP, STP y FTP

Todos estos tipos pertenecen a la categoría 5, que de acuerdo con las normas internacionales pueden trabajar a 100 Mhz, y están diseñados para soportar voz, video y datos. Además de la fibra óptica, que se basa su principal atractivo en estas habilidades.

El UTP es sin duda el que esta ahora ha sido aceptado, por su costo accesible y su fácil instalación. Sus dos alambres de cobre torcidos aislados con plástico PVC, ha demostrado un buen desempeño en las aplicaciones de hoy. Sin embargo a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente.

El STP se define con un blindaje individual por cada par, más un blindaje que envuelve a todos los pares. Es utilizado preferentemente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas. Aunque con el inconveniente de que es un cable robusto, caro y fácil de instalar.

El FTP cuenta con un blindaje de aluminio que envuelve a los pares para dar una mayor protección contra las emisiones electromagnéticas del exterior. Tiene un precio intermedio entre el UTP y DTP y requiere ser instalado por personal calificado.

El cable recto de cobre consiste en alambres de cobre forrados con una aislante. Se usa para conectar varios equipos periféricos en distancias cortas y a bajas velocidades de transmisión. Los cables seriales usados para conectar los modems o las impresoras seriales son de este tipo. Este tipo de alambre sufre de interferencia a largas distancias.

1.3.2.1 Par Trenzado sin Blindar (UTP)

Es el soporte físico más utilizado en las redes LAN, pues es barato y su instalación es barata y sencilla. Por él se pueden efectuar transmisiones digitales (datos) o analógicas (voz). Consiste en un mazo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la Diafonía. Un cable de par trenzado puede tener pocos o muchos pares; en aplicaciones de datos lo normal es que tengan 4 pares. Uno de sus inconvenientes es la alta sensibilidad que presenta ante interferencias electromagnéticas.

En Noviembre de 1991, la EIA (Electronics Industries Association) publicó un documento titulado: Boletín de sistemas técnicos-especificaciones adicionales para cables de par trenzado sin apantallar, documento TSB-36. En dicho documento se dan las diferentes especificaciones divididas por categorías de cable UTP (Unshielded Twisted Pair). También se describen las técnicas empleadas para medir dichas especificaciones por ejemplo, se definen la categoría 3 hasta 16 Mhz, la categoría 4 hasta 20 Mhz y categoría 5, hasta 100 Mhz.

El cable de par trenzado sin blindaje UTP se clasifica según su categoría. Este cable UTP permite la transmisión de grandes volúmenes de información. Estas propiedades están dadas por varios factores: el cobre con que está fabricado el conductor, el material de recubrimiento, tanto de cada conductor como del cable total y finalmente en trenzado de cada par. Estas características hacen que el cable no requiera de blindaje para mantener la señal limpia y estable.

1.3.2.1.1 Categorías del cable UTP

Una categoría de cableado es un conjunto de parámetros de transmisión que garantizan un ancho de banda determinado en un canal de comunicaciones de cable de par trenzado.

La atenuación es un parámetro de transmisión y es la reducción de potencia de la señal, a medida que viaja por el cable, se expresa en términos de dB/100m. A menor gama de dB, el cable es mejor.

El *crosstalk* es causado por las interferencias de los pares adyacentes, en los cables que están incorrectamente apantalladas. Es el traspaso no deseado de una señal de un circuito a otro. La EIA/TIA 568 específica la capacidad de un cable para rechazar las interferencias *crosstalk* desde los pares en extremo más cercano o en el emplazamiento local como el *near-end crosstalk* (NEXT), el cual se expresa en dB. El NEXT Par a Par mide el crosstalk entre cualquiera de los dos pares del cable, A mayor gama de dB, el cable es mejor. La diferencia entre la atenuación y el NEXT es conocido como la relación *atenuación-a-crosstalk* (ACR), Sin embargo la ACR no está citada oficialmente en la EIA/TIA 568, que se dedica más a la capacidad de prestaciones y construcción del cable qua a la relación de la atenuación, El Power Sum NEXT (PS NEXT), una medida más rigurosa del *crosstalk*, mide todo el *crosstalk* posible entre un par y los pares adyacentes en la misma funda del cable. El PS NEXT es el método requerido por la TIA para medir el NEXT en múltiples pares (más de cuatro pares) del cable Backbone. Es una medida critica para las nuevas redes de alta velocidad, La relación del retardo es la diferencia en ns entre el tiempo, cuando el primer y el ultimo bits de un sólo byte paralelo de datos se recibe en el cable. La relación de retardo tampoco está contemplado por la EIA/TIA 568.

Dentro del cableado estructurado las categorías más comunes son:

1. *UTP categoría 1*: La primera categoría responde al cable UTP Categoría 1, especialmente diseñado para redes telefónicas, el clásico cable empleado en teléfonos y dentro de las compañías telefónicas,

2. *UTP categoría 2:* El cable UTP Categoría 2 es también empleado para transmisión de voz y datos hasta 4Mbps,

3. *UTP categoría 3:* La categoría 3 define los parámetros de transmisión hasta 16 MHz. Los cables de categoría 3 están hechos con conductores calibre 24 AWG y tienen una impedancia característica de 100 W. Entre las principales aplicaciones de los cables de categoría 3 encontramos: voz, Ethernet 10Base-T y Token Ring,

Parámetro de transmisión	Valor para el cana a 16 MHz
Atenuación	14.9dB
NEXT	19.3dB
ACR	4.0dB

Tabla 26. Valores de los parámetros de transmisión para UTP categoría 3 que fueron publicados en el documento TSB-67.

4. *UTP categoría 4:* El cable UTP Categoría 4 tiene la capacidad de soportar comunicaciones en redes de datos a velocidades de 20Mbps,

5. *UTP categoría 5:* Es una verdadera norma actual dentro de las redes LAN particularmente, con la capacidad de sostener comunicaciones a 100Mbps. Lo interesante de este último modelo es la capacidad de compatibilidad que tiene contra los tipos anteriores. Sintéticamente los cables UTP se pueden catalogar en una de dos clases básicas: los destinados a comunicaciones de voz, y los dedicados a comunicaciones de

datos en redes. La categoría 5 define los parámetros de transmisión hasta 100 MHz. Inicialmente, la categoría 5 sólo definía atenuación y NEXT como parámetros importantes en la medición de las características del canal. A raíz de los trabajos en Gigabit Ethernet se agregaron nuevos parámetros a la definición de esta categoría puesto que había que garantizar una transmisión por los cuatro pares de manera simultánea en ambas direcciones. Los cables de categoría 5 están hechos con conductores calibre 24 AWG y tienen una impedancia característica de 100 Ω. Entre las principales aplicaciones de los cables de categoría 5 encontramos: voz, Ethernet 10Base-T, Token Ring, 100VG AnyLan, Fast Ethernet 100Base-TX, ATM 155 Mbps, ATM 622 Mbps y Gigabit Ethernet.

Parámetro de transmisión	Valor para el cana a 100 MHz
Atenuación	24dB
NEXT	27.1dB
PSNEXT	NA
ACR	3.1dB
PSACR	NA
ELFEXT	17dB
PSELFEXT	14.4dB
Pérdida de retorno	8dB
Retraso de propagación	548ns
Delay Skew	50ns

Tabla 27. Valores de los parámetros de transmisión para UTP categoría 5 que fueron publicados en el documento TSB-95.

6. *UTP categoría 5 mejorada*: La categoría 5 mejorada define los parámetros de transmisión hasta 100 MHz. La diferencia fundamental con la categoría 5 normal es que los parámetros atenuación, NEXT, y PSELFEXT tienen un margen adicional para garantizar mejor la transmisión de Gigabit Ethernet. Entre las principales aplicaciones de los cables de categoría 5 mejorasda encontramos: voz, Ethernet 10Base-T, Token Ring, 100VG AnyLan, Fast Ethernet 100Base-TX, ATM 155 Mbps, ATM 622 Mbps y Gigabit Ethernet.

Parámetro de transmisión	Valor para el cana a 100 MHz
Atenuación	24dB
NEXT	30.1dB
PSNEXT	27.1dB
ACR	6.1dB
PSACR	3.1dB
ELFEXT	17.4dB
PSELFEXT	14.4dB
Pérdida de retorno	10dB
Retraso de propagación	548ns
Delay Skew	50ns

Tabla 28. Valores de los parámetros de transmisión para UTP categoría 5 mejorada que fueron publicados en la norma TIA/EIA-568A.

7. *UTP Categoría 6:* Soporta frecuencias de 250 Mhz, dos y medio más que las especificaciones que cualquiera de la Categoría 5. El cable de Nivel 6 tiene mejores prestaciones y frecuencias superiores (hasta 155 Mhz contra los 100 Mhz de la Categoría 5). El cableado de Nivel 6 debe cumplir especificaciones más severas para que pueda trabajar en operaciones full-duplex. Cumple con las siguientes especificaciones (en la norma TIA/EIA a 200 MHz):

Parámetro de transmisión	Valor para el cana a 250 MHz
Atenuación	31.2dB
NEXT	34.8dB
PSNEXT	31.9dB
ACR	-3.6dB
PSACR	-0.7dB
ELFEXT	17.2dB
PSELFEXT	14.2dB
Pérdida de retorno	----
Retraso de propagación	547ns
Delay Skew	50ns

Tabla 29. Valores de los parámetros de transmisión para UTP categoría 6.

Para un futuro lejano, el TIA/EIA está buscando la norma de la Categoría 7 con el ancho de banda de 600Mhz. Se sabe que la Categoría 7 va a usar una nueva interface, la cual todavía no está determinada. Es una nueva generación de cables que promete al menos el doble de ancho de banda del Cable Categoría 5. El cable de Nivel 7 debe poder soportar Gigabit Ethernet a 100 m, alcanzar al menos 10 dB en ACR a 200 Mhz, y soportar niveles de PS NEXT superiores a los de los cables de Nivel 6.

1.4 Dispositivos de Interconexión de red

1.4.1 Repetidores

El propósito de un repetidor es regenerar y temporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios. Los repetidores son equipos que trabajan en la capa física del modelo OSI, es decir, repiten todas las señales de un segmento a otro a nivel eléctrico. Operan amplificando todas las señales eléctricas que reciben, es decir, son transparentes hasta los protocolos más altos. No proporciona ningún tipo de aislamiento entre redes. Sólo pueden proporcionar una gestión de redes planas.

Se emplean para ampliar el alcance geográfico de una red, conectando dos o más LANs.

Su mayor ventaja es poder conectar redes con diferente medio de transmisión, por ejemplo, Ethernet sobre UTP a Ethernet sobre fibra óptica. Más que repetidores lo que se suele utilizar son regeneradores que no solo amplifican, sino que devuelven la señal digital original eliminando el ruido.

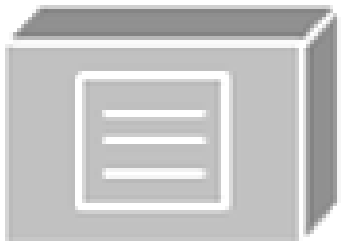


Figura 38. Diagrama Lógico de un Repetidor.

1.4.2 Concentradores o Hubs

El término concentrador se utiliza a veces para referirse a una pieza de equipo de red que conecta hosts entre sí, aunque realmente es un repetidor multipuerto. Se llama así porque pasa o repite toda la información que recibe a todos sus puertos.

Los concentradores se pueden utilizar para ampliar una red. No obstante, de esta acción puede resultar un exceso de tráfico innecesario porque se envía la misma información a todos los dispositivos de una red.

Los concentradores están indicados para redes pequeñas, aunque las redes con alta carga de tráfico necesiten equipos de interconexión de red adicionales, como puede ser un switch o un enrutador, que reducirían el tráfico innecesario.

Las propiedades de un concentrador son las siguientes:

- Hay un solo dominio de broadcast
- Ancho de banda compartido o *bandwidth domain*
- Amplifican señales
- Propagan señales a través de la red
- No necesitan filtrarse
- No requieren determinación de ruta
- Se utilizan como puntos de concentración de la red

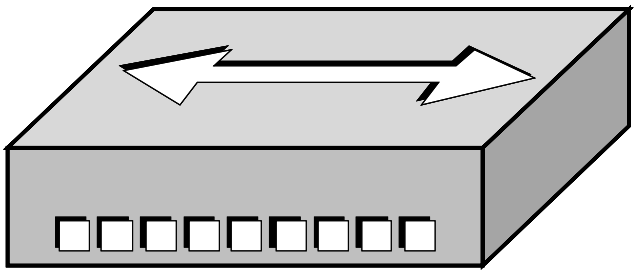


Figura 39. Diagrama Lógico de un Concentrador o Hub.

1.4.3 Bridges o Bridges

Un bridge es un dispositivo usado para interconectar redes de área local (LAN). Los bridges reciben todas las tramas enviadas por cada red acoplada a él, y los reenvía selectivamente entre las LANs, utilizando solo las direcciones de capa 2 (capa de enlace) para determinar donde retransmitir cada trama. Los bridges reenvían solo aquellas tramas que están destinadas a un host del otro lado del bridge, descartando aquellos que no necesitan ser retransmitidos.

Los bridges locales conectan LANs, las cuales no están colocadas en sitios diferentes. Por ejemplo, aquellas que son adyacentes a lo largo de su longitud. Los bridges locales permiten a un edificio grande o campus compacto tener una única red lógica, más larga que la que podría ser con un solo segmento de cable y proporciona aislamiento eléctrico y de tráfico entre segmentos.

Los bridges remotos conectan LANs de lugares distantes. Estos bridges se usan en pares, cada bridge remoto se conecta a una LAN y a otro bridge remoto mediante un enlace. Como los bridges no necesitan tener enlaces con la misma velocidad en ambos lados, pueden ser utilizados para interconectar LANs vía enlaces de radiofrecuencia de baja velocidad.

La mayoría de los bridges actuales son capaces de aprender automáticamente la topología de la red (*learning bridges*), examinando cada trama que reciben anotando la dirección fuente de tales tramas. Cualquier dirección fuente que el bridge no haya visto antes, será almacenada en su tabla interna para referencias futuras.

Cuando un bridge recibe de un host una trama que tiene una dirección destino desconocida, envía la trama a todas los otros puertos para asegurar que la trama alcanzará su destino. En el futuro cualquier trama recibida de ese host como destino, el bridge conocerá su localización.

Los bridges proporcionan mejoras de tráfico y aislamiento que los repetidores entre segmentos de LAN, pero introducen algún retardo. Pero no dan el alto grado de aislamiento de tráfico entre LANs.

1.4.3.1 Bridges Multipuerto

Los bridges multipuerto son bridges con tres o más interfaces de enlace de datos o puertos. Se utilizan para conectar más de dos LAN en un único punto. Normalmente tienen mejores prestaciones que los convencionales bridges de dos puertos.

Como resultado del mayor número de puertos y mejores prestaciones, un único bridge multipuerto puede ser usado para reemplazar varios bridges de dos puertos conectados conjuntamente por medio de segmentos LAN.

El bridge multipuerto también proporciona mejores prestaciones debido a que las tramas son conmutadas de una LAN a otra sobre su bus Entrada/Salida o su memoria, las cuales son mucho más rápidas que los segmentos de LAN.

La operación de los bridges multipuerto es superior en el sentido de filtrar y reenviar tramas, con la excepción de que la determinación de a donde deben ser enviados tales tramas es más compleja. Después que la dirección de una trama ha sido filtrada para saber si debe ser retransmitida la trama, el bridge multipuerto decide a través de cual puerto debe ser enviada. Cuando se recibe una trama con dirección desconocida, broadcast o multicast, el bridge multipuerto lo transmitirá sobre todas sus conexiones excepto por la que llegó.

Las características principales de un bridge son:

- Ancho de banda compartido o *bandwidth domain*
- Un solo dominio de broadcast

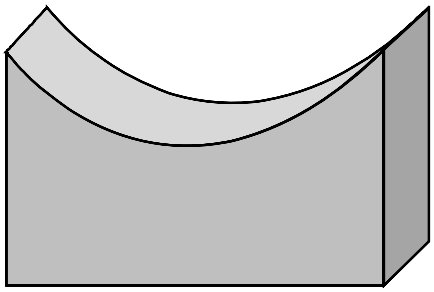


Figura 40. Diagrama Lógico de un Bridge.

1.4.4 Switches o Comutadores LAN

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y cuellos de botella. Puede agregar mayor ancho de banda, acelerar la salida de tramas, reducir tiempo de espera y bajar el costo por puerto. El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada host. Los switches utilizan la información de la dirección de cada trama para controlar el flujo del tráfico de la red. Por medio de la monitorización de las tramas que recibe, un switch distingue qué dispositivos están conectados a sus puertos, y envían las tramas a los puertos adecuados solamente. Opera en la capa 2 (capa de enlace) del modelo OSI y reenvía las tramas en base a la dirección MAC.

Reduce la cantidad de tráfico innecesario porque la información recibida en un puerto se envía solamente al host que tiene la dirección destino correcta, a diferencia de un concentrador, que la envía a todos los puertos. Los switches no están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo. Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada host compita por el medio, dando a cada uno de ellos un ancho de banda comparativamente mayor.

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre la arquitectura Cliente/Servidor, pues los usuarios juzgan la red por la rapidez de obtener la información y la confiabilidad del servicio.

Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- El elevado incremento de hosts en la red.
- El continúo desarrollo de procesadores más rápidos y poderosos en los hosts.
- La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones basadas en la arquitectura Cliente/Servidor, como aplicaciones multimedia (*Streaming*, Bases de datos, Servidores de archivos, etc.)
- La tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.
- El desarrollo de audio y video sobre IP (H.323, H.324, VoIP, etc.)

Las características más importantes de un switch son:

- Varios dominios de colisión
- Varios dominios de ancho de banda
- Un solo dominio de broadcast, a menos que se utilicen VLANs
- La capacidad de microsegmentar con VLANs y el uso de troncales (802.1Q)
- El uso de protocolos para autentificar a nivel de capa 2 (802.1x), entre otros
- Multicapa

Los switches resuelven los problemas de anchos de banda al segmentar un dominio de colisiones de una LAN, en pequeños dominios de colisiones.

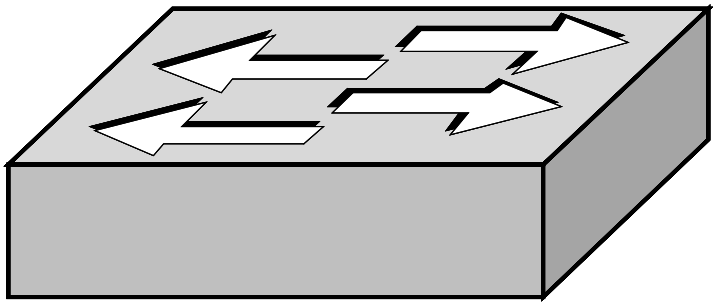


Figura 41. Diagrama Lógico de un Switch.

1.4.4.1 Spanning Tree (802.1d)

La mayoría de los administradores de red subestimaron la importancia del Protocolo Spanning Tree (STP). Debido a que los enrutadores se volvieron populares al inicio de los años 90s, STP quedo como un protocolo de menor importancia pasando a segundo termino, lo único que tenia que hacer era solo trabajar. Sin embargo, ahora, con el reciente auge de la tecnología basada en la conmutación, *Spanning Tree* se ha convertido en un factor de mayor importancia que tiene un tremendo impacto en el desempeño de las redes. Es un hecho que STP a menudo es responsable de más del 50% de la configuración, resolución de problemas y mantenimiento que dan dolores de cabeza en el mundo real a las redes pobremente diseñadas. STP es un protocolo muy complejo que no ha sido entendido en su totalidad, se tiene la dificultad de que existe poca información de

buena calidad, especialmente información a cerca de modernas implementaciones de STP.

1.4.4.1.1 Definición y Uso de Spanning Tree

En el más básico sentido, *Spanning-Tree Protocol* (STP) es un protocolo que previene los loops. Es una tecnología que permite a los bridges comunicarse con otros bridges para descubrir los loops físicos en una red. El protocolo, entonces, especifica un algoritmo que los bridges pueden usar para crear una topología lógica libre de loops. En otras palabras, STP crea una topología de árbol libre de loops a nivel de capa 2. Los loops ocurren en las redes por diversas razones. La razón más común que provoca loops en una red es el intento deliberado de proveer redundancia a la red (en el caso de que un enlace o un switch fallen, otro enlace u otro switch pueden hacer el trabajo). Sin embargo, los loops también pueden ocurrir por errores. En la siguiente figura se muestra una típica red basada en switches y como los loops son utilizados intencionalmente para proveer redundancia a la red.

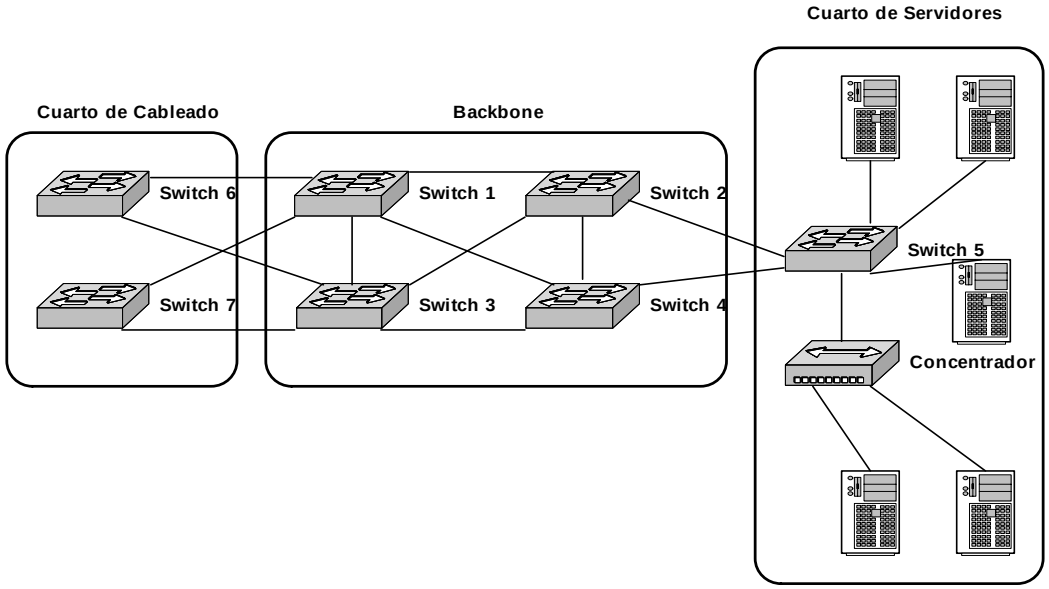


Figura 42. Las redes a menudo incluyen loops para proveer redundancia.

El problema es que los loops son potencialmente desastrosos en una red basada en switches, las dos razones importantes son: los loops de broadcast y la corrupción en la tabla del bridge.

1.4.4.1.1.1 Loops de Broadcast

Los broadcasts y loops de capa 2 pueden ser una peligrosa combinación. Considerando la Figura No. 6.

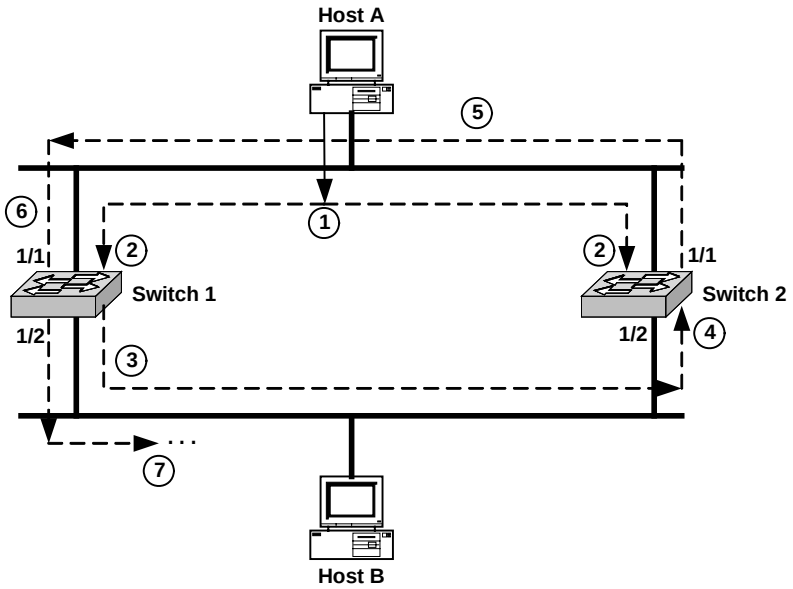


Figura 43. Sin STP, los broadcasts crean loops de realimentación.

Asumiendo que ninguno de los switches están corriendo STP. El Host A comienza por enviar una trama a la dirección MAC de broadcast (FF-FF-FF-FF-FF-FF) en el paso 1. Ya que Ethernet tiene como medio un bus, esta trama viaja tanto al switch 1 como al switch 2 (paso 2).

Cuando la trama arriva al switch 1: puerto 1/1, el switch 1 seguirá el algoritmo normal de bridgeo y enviara la trama por el puerto 1/2 (paso 3). Nuevamente, esta trama viajara hacia todos los nodos en los segmentos Ethernet más bajos, incluyendo el switch 2: puerto 1/2 (paso 4), El switch 2 enviara la trama por el puerto 1/1 (paso 5) y, una vez más, la trama será vista por el switch 1: puerto 1/1 (paso 6). El switch 1, siendo un buen switch, seguirá ordenes y enviara la trama hacia fuera del puerto 1/2 por segunda vez (paso 7). Viendo el patrón que se sigue se puede tener en cuenta que se esta en presencia de un loop.

Adicionalmente, se debe tener en cuenta que se esta ignorando la trama que arrivo al switch 2: puerto 1/1 en el paso 2. Esta trama también será enviada hacia los segmentos Ethernet de abajo y creará un loop en dirección contraria al anterior. En otras palabras, no olvidar que este loop de retroalimentación ocurrirá en ambas direcciones.

Notando una importante conclusión en lo explicado anteriormente se puede ver que los loops de bridges son más peligrosos que los loops de enrutamiento. Por ejemplo la trama de Ethernet DIX V2 contiene dos campos de dirección MAC, un campo de tipo y una de CRC, por el contrario el encabezado de IP contiene el campo de *time to live* (TTL) que viene con un valor desde el host original y este se va decrementando a medida que va pasando por cada enrutador. Descartando los paquetes que tengan un TTL=0, esto permite a los enrutadores prevenir paquetes que sigan en la red. Ethernet no tiene un campo para TTL. Por lo tanto, después de que una trama comienza un loop en la red del ejemplo, esta continúa por siempre hasta que alguien apaga un switch o rompe un enlace. Las redes que son más complejas que la ilustrada en la Figura 2, pueden causar que el

loop de retroalimentación crezca de manera exponencial, debido a que la trama es enviada hacia fuera de todos los puertos de los switches, el número total de las tramas aumenta rápidamente. Finalmente, si se considera el impacto que provoca esta tormenta de broadcast para los usuarios de los hosts A y B en la Figura 6. Estos no podrán hacer nada, ya que los broadcasts deben ser procesados por todos los CPUs de los dispositivos conectados en los segmentos de red y si se tiene toda una tormenta de broadcast, literalmente se consumirá el 100% del CPU y los hosts quedarán pasmados, aún si se apaga algún host, este volverá a trabajar con normalidad pero una vez que sea conectado nuevamente a la red pasará lo mismo.

1.4.4.1.1.2 Corrupción en la tabla de Bridging

Muchos de los administradores son concientes del problema que provocan las tormentas de broadcast. Sin embargo, muy poca gente es conciente del hecho de que también las tramas de unicast pueden circular por siempre en una red que contiene loops. En la Figura 44 se ilustra este punto.

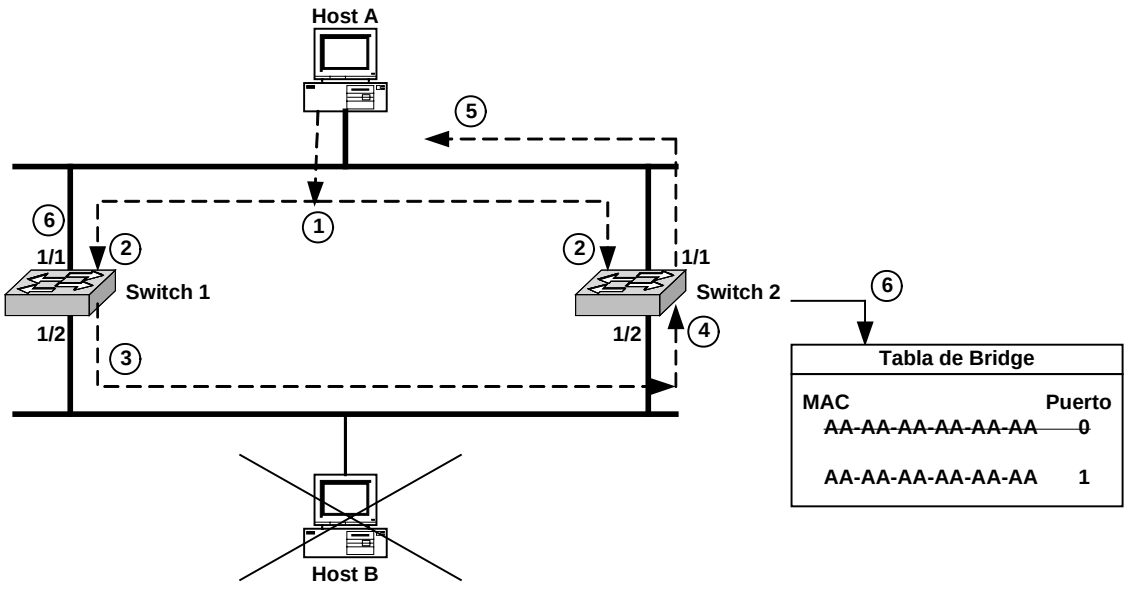


Figura 44. Sin STP, también las tramas de unicast pueden provocar loops y corromper la tabla de bridge.

Por ejemplo, suponiendo que el host A, que posee una entrada de ARP con más prioridad para el host B, quiere mandar un paquete ping de unicast hacia el host b. Sin embargo, el host B ha sido removido temporalmente de la red y la correspondiente entrada para la tabla de bridge en los switches ha sido borrada para el host B. Si ambos switches no están corriendo STP. Y como en el ejemplo anterior, las tramas viajan hacia el puerto 1/1 de ambos switches (Paso 2), el texto solo considera las cosas desde el punto de vista del switch 1. Dado que el host B esta apagado, el switch 1 no tiene entrada para la dirección MAC BB-BB-BB-BB-BB-BB en su tabla de bridge, por lo tanto el switch 1 desecha la trama (paso 3). En el paso 4, el switch 2 recibe la trama en le puerto 1/2. Dos eventos (ambos malos) pueden pasar en este punto:

1. Que el switch 2 deseche la trama debido a que él nunca aprendió la dirección MAC BB-BB-BB-BB-BB-BB (paso 5). Esto crea un loops de retroalimentación y debilita el funcionamiento en la red.
2. El switch 2 nota que acaba de recibir una trama en el puerto 1/2 con la dirección MAC fuente AA-AA-AA-AA-AA-AA. El switch 2 cambia su entrada para la dirección MAC del host A hacia el puerto equivocado.

Como las tramas fluyen en dirección contraria (recordando que los loops de retroalimentación existen en ambas direcciones), se ve que la dirección MAC del host A está apareciendo entre el puerto 1/1 y el puerto 1/2.

No solo se satura permanentemente la red con los paquetes ping de unicast, además se corrompen las tablas de bridge. Recuerda ahora que no solo los broadcasts pueden arruinar la red.

1.4.4.1.2 Conceptos Clave de Spanning-Tree Protocol

Los cálculos de Spanning Tree hacen un uso extensivo de dos conceptos clave cuando crean una topología lógica libre de loops:

- Bridge ID (BID)
- Path Cost

1.4.4.1.2.1 Bridges IDs

El bridge ID es un simple campo de 8 bytes que esta compuesto por dos subcampos como se ilustra en la Figura 45.

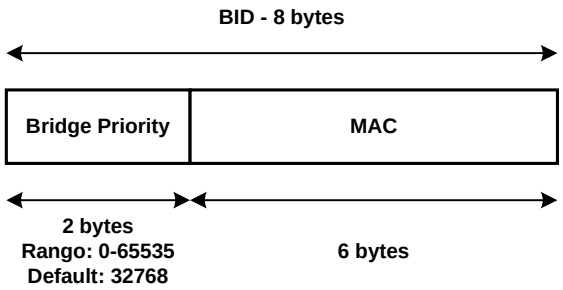


Figura 45. El bridge ID se compone de la prioridad de bridge y de una dirección MAC.

El subcampo de orden bajo consiste de una dirección MAC de 6 bytes asignada al switch. Este es un número codificado que es diseñado para que no pueda ser cambiado por el usuario. La dirección MAC en el BID es expresada en formato hexadecimal (base 16).

El subcampo de orden alto es conocido como prioridad de bridge, es de un valor 2 bytes (16 bits). Un entero de 16 bits sin signo puede tener 2^{16} posibles valores en el rango 0-65535. El valor por omisión para la prioridad de bridge es el valor medio, 32768. La prioridad de bridge, es usualmente expresado en formato decimal (base 10).

1.4.4.1.2.2 Path Cost

Los bridges usan el concepto de costo para evaluar que tan cerca están ellos de otros bridges. La norma 802.1d originalmente definió el concepto de costo como 1000 Mbps divido entre el ancho de banda del enlace en Mbps. Por ejemplo, un enlace de Ethernet 10baseT tiene un costo de 100 (1000/10), Fast Ethernet y FDDI usan un costo de 10 (1000/100). Este esquema ha servido muy bien desde que Radia Perlman comenzó a trabajar con el protocolo en 1983. Sin embargo, con el crecimiento de Gigabit Ethernet y OC-48 ATM (2.4 Gbps), se tuvieron problemas ya que el concepto de costo fue establecido como un valor entero que no permite costos fraccionales. Por ejemplo, OC-48 ATM tiene 1000 Mbps/2400 Mbps=.41667, que es un valor invalido para el concepto de costo. Una solución es usar un costo de valor 1 para todos los enlaces iguales o mayores a 1 Gbps; sin embargo, esto impide que STP escoja precisamente el mejor camino en las redes Gigabit.

Como solución para este problema, la IEEE ha decidido modificar el costo para usar una escala no lineal. La tabla 30 enlista los nuevos valores de costo.

Ancho de Banda	Costo STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Tabla 30. Valores de costo STP para redes que usan bridges.

Los valores de la Tabla 26 fueron escogidos cuidadosamente para que los viejos y nuevos esquemas ínter operaran con las velocidades de los enlaces en uso común en estos días.

El punto clave que se debe de recordar en lo que respecta a los valores de costos STP es que los costos de valor menor son mejores.

1.4.4.1.3 Cuatro Pasos para la Secuencia de Decisión de STP

Cuando se crea una topología lógica libre de loops, Spanning Tree siempre usa la misma secuencia de decisión de cuatro pasos:

Paso 1. El menor BID Raiz
Paso 2. El menor Path Cost para el Bridge Raiz
Paso 3. El menor BID transmisor
Paso 4. El menor ID de puerto

Los bridges intercambian información Spanning Tree entre ellos mismos usando tramas especiales conocidos como *Bridge Protocol Data Units* (BPDUs). Un bridge usa esta secuencia de decisión de cuatro pasos para salvar una copia del mejor BPDU visto en todos los puertos. Cuando hace esta evaluación, el bridge considera a todos los BPDUs recibidos en el puerto como el BPDU que puede ser enviado por ese puerto. Cuando los BPDU llegan, son revisados con esta secuencia para ver si es más atractivo (esto es, el de menor valor) que el BPDU salvado en ese puerto. Si el nuevo BPDU (o el BPDU generado localmente) es más atractivo, el valor viejo es reemplazado.

Además, el proceso de salvar el mejor BPDU también controla el envío de los BPDUs. Cuando un bridge se convierte en el primer bridge activo, todos sus puertos están enviando BPDUs cada 2 segundos (cuando están usando el valor de contador por omisión). Sin embargo si un puerto escucha otro BPDU proveniente de otro bridge que es más atractivo que el BPDU que ha estado enviando, el puerto local para el envío de BPDUs. Si el BPDU más atractivo para el arrivo desde el switch vecino por un periodo de tiempo (20 segundos por omisión), el puerto local puede una vez más continuar con el envío de BPDUs.

1.4.4.1.4 Tres pasos para la Convergencia Inicial STP

Aunque hay muchas facetas para el STP, la convergencia inicial puede ser descompuesta en tres pasos simples:

Paso 1. Elección de Bridge Raiz
Paso 2. Elección de Puertos Raiz
Paso 3. Elección de Puertos Designados

Cuando la red inicia, todos los bridges están anunciando una mezcla caótica de información BPDU. Sin embargo, los bridges inmediatamente comienzan a aplicar la secuencia de decisión de cuatro pasos. Esto permite que los switches se agrupen con el arreglo de BPDUs en un simple árbol de expansión para toda la red. Un solo bridge Raiz es elegido para actuar como “el centro del universo” para esta red (paso 1). Todos los bridges restantes calculan un arreglo de puertos raíz (paso 2) y de puertos designados (paso 3) para construir una topología libre de loops. Podemos imaginarnos a la topología resultante como una llanta: El bridge Raíz es el concentrador con caminos activos libres de loops radiando hacia fuera. En estado de equilibrio de la red, los BPDUs fluyen exteriormente desde el bridge Raíz por todos los caminos activos libres de loops hacia todos los segmentos de la red.

Después de que la red ha convergido en una topología activa libre de loops utilizando este proceso de tres pasos, los cambios adicionales son manejados usando el proceso de Cambio de Topología.

Para la discusión que sigue en el resto del tema, se debe tomar como referencia la Figura 46 como la presentación de un modelo de una red de tres switches/bridges.

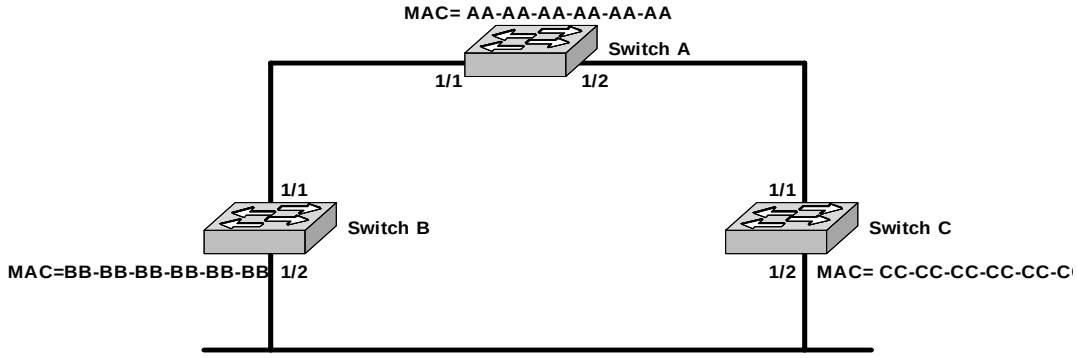


Figura 46. Modelo de Red Presentado para la discusión de las operaciones básicas STP.

Esta red consiste de tres switches conectados en una configuración enlazada. A cada switch se le ha asignado una dirección MAC ficticia que corresponde al nombre del equipo (por ejemplo, switch A usa la dirección MAC AA-AA-AA-AA-AA-AA).

1.4.4.1.4.1 Paso 1: Elección de Bridge Raíz

Los switches primero tienen que elegir un bridge Raíz buscando el bridge con el menor BID. Se puede ver que el switch A tiene un BID por default de 32768.AA-AA-AA-AA-AA-AA. Nótese la mezcla de la prioridad de bridge decimal y la dirección MAC hexadecimal. A pesar de que esto posiblemente se vea un poco raro, esta convención te permite ver cada sección del BID en su formato más común.

Continuando con el ejemplo, el switch B asume un BID por default de 32768.BB-BB-BB-BB-BB-BB, y el switch C usa 32768.CC-CC-CC-CC-CC-CC. Dado que los tres switches están usando el valor de prioridad de bridge por omisión, la dirección MAC más baja (AA-AA-AA-AA-AA-AA) sirve para romper el empate, y el switch A se convierte en el bridge Raíz. La Figura 47 ilustra este proceso.

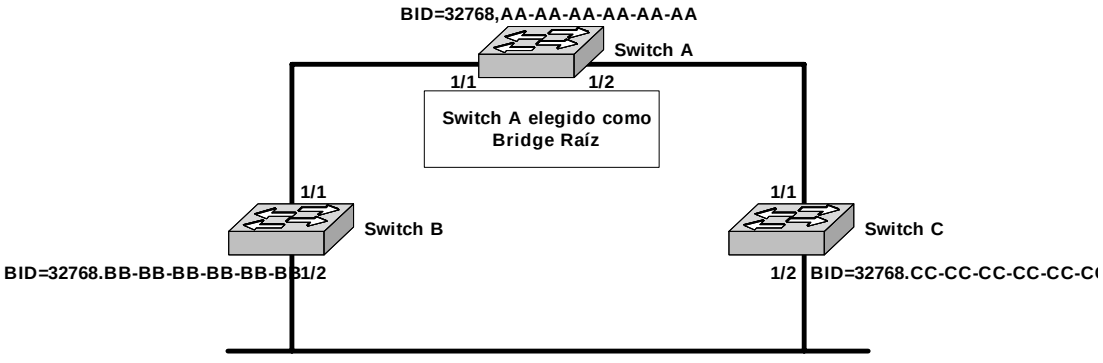


Figura 47. La red debe elegir un solo Bridge Raíz.

Esto esta bien, pero como los switches saben que el switch A tiene el menor BID. Esto es realizado a través del cambio de BPDUs. Por omisión los BPDUs son emitidos cada 2 segundos. Los BPDUs son tráfico entre bridges, ellos no contienen nada de tráfico de los usuarios finales. La Figura 48 ilustra la presentación básica de un BPDU.

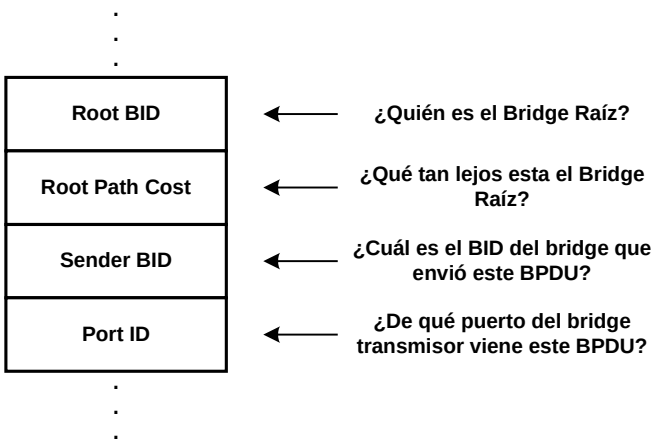


Figura 48. Presentación básica de un BPDU.

Cuando un bridge genera BPDUs cada 2 segundos, el piensa que es el bridge Raíz y coloca ese instante de tiempo en el campo de BID Raíz. El bridge siempre coloca su propio BID en el campo de BID emisor.

Cuando un bridge inicia por primera vez, siempre coloca su BID tanto en el campo de BID Raíz como en el de emisor BID. Suponiendo que el switch B inicia primero y comienza a enviar BPDUs cada 2 segundos anunciándose como el bridge Raíz. Unos minutos después el switch C inicia anunciando como bridge Raíz por si mismo. Cuando el BPD del switch C arriva al switch B, el switch B descarta el BPDU porque el tiene un menor BIP guardado en sus puertos (su propio BID). Tan pronto como el switch B transmite un BPDU, el switch C aprende que este BPDU no es tan importante como el que tomo primero. En este momento, El switch C comienza a enviar BPDUs que enlistan al switch B como el BID Raíz y al switch C como el BID transmisor. La red ahora esta de acuerdo en que el switch B es el bridge Raíz.

Cinco minutos después el switch A inicia. Como lo visto anteriormente con el switch B, El switch A asume que él es el bridge Raíz y comienza a advertir este hecho por medio de BPDUs. Tan pronto como estos BPDUs llegan a los switches B y C, estos adjudican la posición de bridge Raíz al switch A. Todos ellos ahora están enviando BPDUs que anuncian que el bridge Raíz es el switch A y a ellos mismos como el transmisor BID.

1.4.4.1.4.2 Paso 2: Elección de Puertos Raíz

Después de elegir un bridge Raíz, los switches continúan con la elección de los puertos Raíz. Un puerto Raíz de un bridge es el puerto que esta más cerca del bridge Raíz. Todos los switches que no son bridge Raíz deben elegir un Puerto Raíz.

Los bridges usan el concepto de costo para juzgar la cercanía entre ellos. Específicamente, los bridges utilizan el concepto llamado *Root Path Cost*, que es el costo acumulado de todos los enlaces hacia el bridge Raíz. La Figura 49 ilustra como se calcula este valor a través de los switches, resultando el proceso de elección del Puerto Raíz.

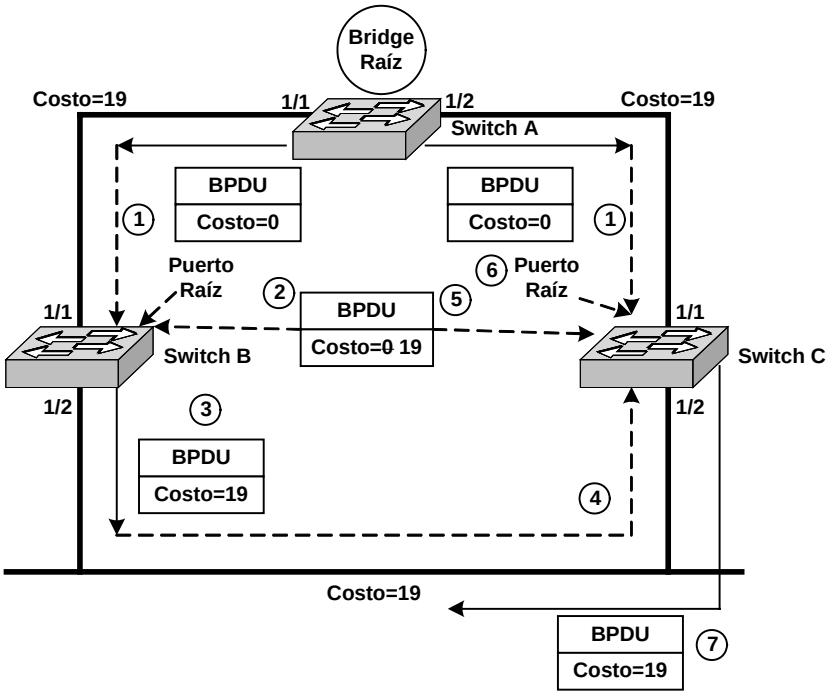


Figura 49. Todos los switches que no son bridge Raíz deben seleccionar un Puerto Raíz.

Cuando el switch A (el bridge Raíz) envía BPDUs, estos contienen un valor de Root Path Cost igual a 0 (Paso 1). Cuando el switch B recibe estos BPDUs, el suma el Path Cost del puerto 1/1 a el *Root Path Cost* contenido en el BPDU recibido. Si en la red hay un switch Catalyst 5000 y todos los enlaces son Fast Ethernet. El switch recive un Root Path Cost igual a 0 y le suma el costo del puerto 1/1 igual a 19 (Paso 2). El switch B usa internamente el valor de 19 y envía BPDUs con un valor de Root Path Cost igual a 19 por su puerto 1/2 (Paso 3).

Cuando el switch C recibe estos BPDUs provenientes del switch B (Paso 4), este incrementa el valor a 38. Sin embargo, El switch C también esta recibiendo BPDUs provenientes del bridge Raíz por el puerto 1/1. Estos entran al switch C: Puerto 1/1 con un costo de 0, y el switch C incrementa internamente este valor a 19 (Paso 5). El switch C tiene que tomar una decisión ahora: debe de elegir un Puerto Raíz, el puerto más cercano al bridge Raíz. El switch C tiene un *Root Path Cost* de 19 en el puerto 1/1 y un *Root Path Cost* de 38 en el puerto ½, por lo tanto el puerto 1/1 se convierte en el Puerto Raíz (Paso 6). El switch C comienza a anunciar a todos los demás switches este valor de 19 para el *Root Path Cost* (Paso 7).

El switch B hace cálculos similares: el puerto 1/1 tendrá un *Root Path Cost* de 19, mientras que el puerto 1/2 calcula uno de 38, por lo tanto el puerto 1/1 se convierte en el puerto Raíz para el switch B. Nos debemos de dar cuenta que el valor del Costo es incrementado cuando los BPDUs son recibidos en un Puerto.

1.4.4.1.4.3 Paso 3: Elección de los Puertos Designados

En la parte para la prevención de loops en el STP viene el tercer paso de la Convergencia Inicial: Elección de los Puertos Designados. Cada segmento en una red que utiliza switches tiene un Puerto Designado. Este funciona como un solo puerto bridge que envía y recibe trafico para y desde el bridge Raíz sobre su segmento de Red. La idea es que si cada puerto maneja trafico para cada enlace, todos los loops serán rotos. El switch que contiene el Puerto Designado para un segmento dado es conocido como el bridge Designado para ese segmento.

Al igual que la selección del puerto Raíz, los Puertos Designados son elegidos gracias a la suma del *Root Path Cost* hacia el bridge Raíz (Figura 50).

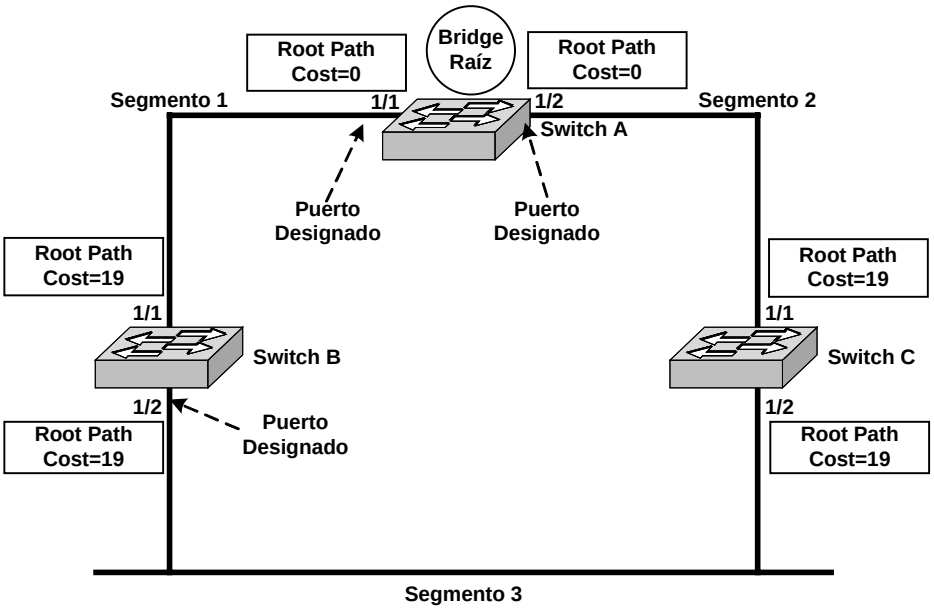


Figura 50. Cada Segmento elige un Puerto Designado basándose en el más bajo Costo.

Para localizar cada Puerto designado, verificar cada segmento en turno. Primero al segmento 1 entre el switch A y el switch B. Se tienen dos puertos bridge en este segmento: switch A: puerto 1/1 y switch B: puerto 1/1. El puerto 1/1 del switch A tiene un *Root Path Cost* igual a 0, debido a que es el bridge Raíz, mientras que el puerto 1/1 del switch B tiene un *Root Path Cost* de 19. Como el puerto 1/1 del switch A tiene el menor valor de *Root Path Cost*, este se convierte en el Puerto Designado para este enlace.

Para el segmento 2 (el enlace entre el switch A y C), ocurre un proceso de elección similar. El puerto 1/2 del switch A tiene un *Root Path Cost* de 0, mientras que le puerto 1/1 del switch C tiene un valor de 19. Como el Puerto 1/2 del switch A tiene un valor menor, este se convierte en el Puerto Designado. Se puede notar que cada puerto activo en el bridge Raíz se convierte en Puerto Designado. La única excepción a esta regla es el loop físico de capa 1 para el bridge Raíz (por ejemplo, si se conectan dos puertos del bridge Raíz al mismo concentrador es como si se conectaran dos puertos con un cable cruzado).

Verificando el segmento 3 (el enlace entre el switch B y C). Tanto el puerto 1/2 del switch B como el puerto 1/2 del switch C tiene un valor de 19 en el *Root Path Cost*, por lo tanto hay un empate. Cuando STP se encuentra con un empate (u otro caso no determinado), STP siempre usa la Secuencia de Decisión de Cuatro Pasos. Como tenemos un empate, esto pone a BID como el tercer criterio de decisión. Como el BID del switch B (32768.BB-BB-BB-BB-BB-BB) es menor que el BID del switch C (32768.CC-CC-CC-CC-CC-CC), el puerto 1/2 del switch B se convierte en el Puerto Designado para el enlace 3. Por consiguiente el puerto 1/2 del switch C se convierte en un Puerto No Designado.

1.4.4.1.5 Los Cinco Estados STP

Después de que los switches han clasificado a sus puertos como Raíz, Designado o No Designado, creando una topología libre de loops: Los puertos Raíz y Designado envían tráfico mientras que los Puertos No designados lo bloquean. A pesar de que el envío y el bloqueo de tráfico son los dos estados comúnmente vistos en una red estable, la Tabla 31 ilustra que hay actualmente 5 estados STP:

Estado	Propósito
Forwarding	Envía y recibe todos los paquetes que ingresan en el puerto.
Learning	Aprende direcciones MAC con las que construye sus tablas, pero no reenvía paquetes.
Listening	Atiende BPDUs para asegurarse de que no hay bucles antes de comenzar a enviar.
Blocking	Recibe BPDUs, pero no envía tramas. Todos los puertos están bloqueados por defecto.
Disable	Administrativamente apagado

Tabla 31. Estados STP.

Esta lista se puede ver como una jerarquía en la cual los puertos bridge inician desde abajo (Deshabilitado o Bloqueado) y trabajan para llegar a *Forwarding*. El estado de Deshabilitado permite a los administradores de red apagar manualmente un puerto. Después de iniciar el sistema, los puertos comienzan en el estado de Bloqueo donde ellos están en espera de BPDUs.

Una variedad de eventos pueden provocar que el switch pase al estado de Listening (pensar que un switch es el bridge Raíz inmediatamente después que fue encendido o el ascenso de BPDUs en cierto periodo de tiempo). Hasta este punto no han pasado datos de usuario, el puerto esta enviando y recibiendo BPDUs en esfuerzo para determinar la topología activa en la red. Es durante el estado de *Listening* en que los tres pasos de

convergencia inicial toman lugar. Los puertos que pierden la elección de Puertos Designados se convierten en Puertos No Designados y regresan al estado de Bloqueo.

Los puertos que permanecen como Puertos Designados y Raíz después de 15 segundos (el valor de tiempo por omisión) progresan hacia el estado de *Learning*. Este es un segundo periodo de 15 segundos donde el switch no esta pasando tramas de datos de los usuarios. En vez de eso, el switch esta construyendo su tabla de bridge. Cuando un switch recibe tramas, este pone la dirección MAC fuente y el puerto de llegada en la tabla de bridge. El estado de *Learning* reduce la gran cantidad de *flooding* requerida cuando el envío de datos inicia.

Si un puerto es aun un Puerto Designado o Raíz al final del estado de *Learning*, el puerto pasa al estado de *Forwarding*. En esta etapa finalmente el puerto inicia la transmisión y recepción de tramas de datos de los usuarios. La Figura 51 ilustra los estados del Puerto y las posibles transiciones.

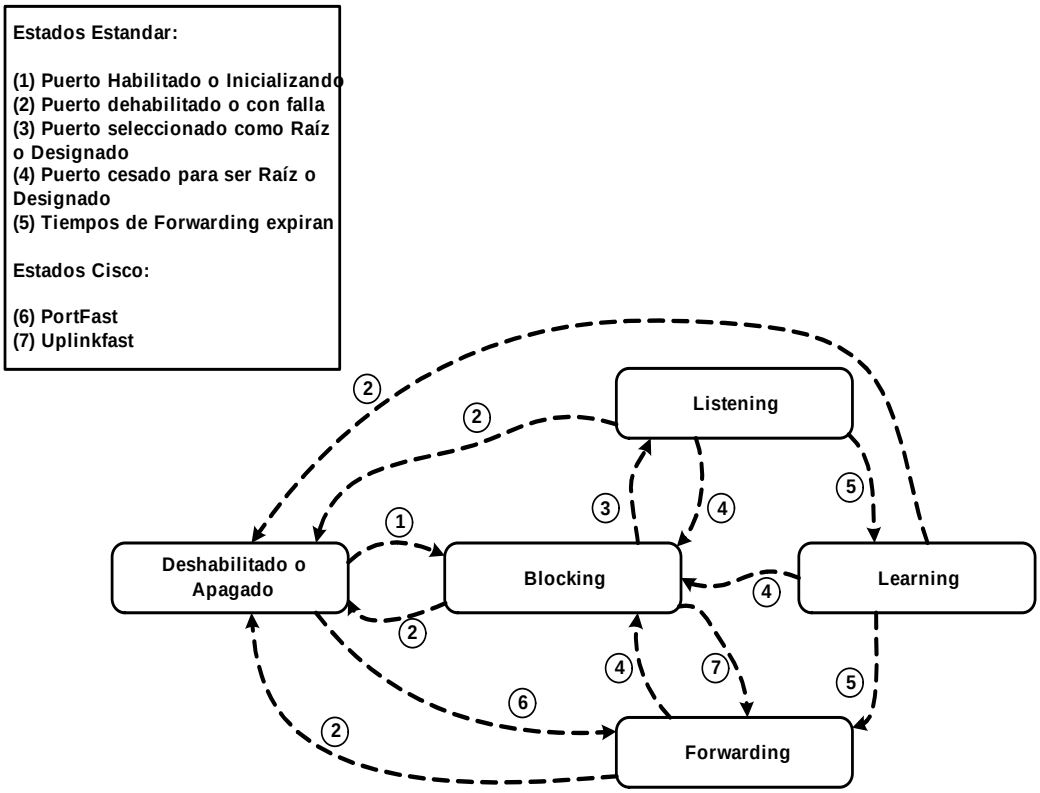


Figura 51. Estados posibles del Puerto y Transiciones.

La Figura 52 muestra la red de ejemplo con sus puertos clasificados y sus estados. Notando que todos lo puertos están en estado de *Forwarding*, excepto el puerto 1/2 del switch C.

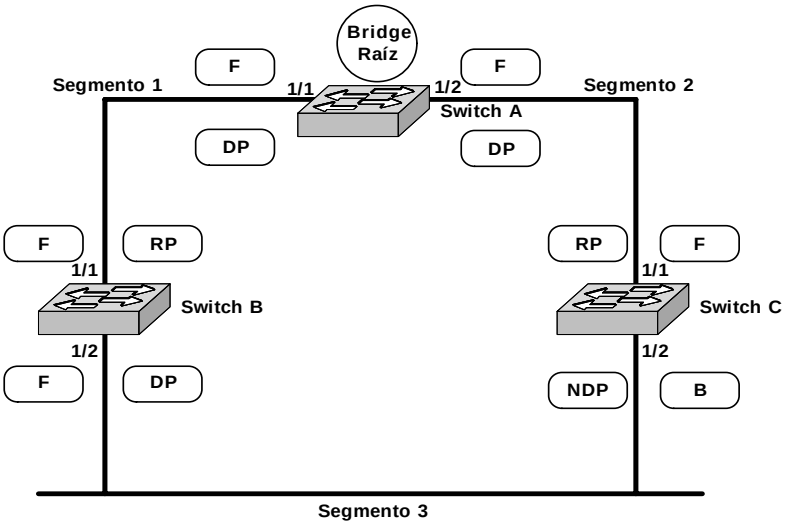


Figura 52. Red de ejemplo con los estados de puertos identificados.

La Tabla 32 enuncia la simbología utilizada para representar los Estados *Spanning Tree*.

Estado del Puerto	Simbolo
Blocking	B
Forwarding	F
Puerto Designado	DP
Puerto Raíz	RP
Puerto No designado	NDP

Tabla 32. Símbolos para los estados de los puertos.

1.4.4.1.6 Los Tres Tiempos para STP

Se ha mencionado que un bridge espera 15 segundos por omisión en los estados de *Listening* y *Learning*. En general. El protocolo Spanning Tree es controlado por los tres tiempos que se enuncian en la tabla 33.

Tiempo	Propósito importante	Default
Hello Time	Tiempo para el envío de BPDUs de configuración por el Bridge Raíz	2 segundos
Forward Delay	Duración de los estados de Learning y Listening	15 segundos
Max Age	Tiempo para BPDU guardado	20 segundos

Tabla 33. Tiempos STP.

El parámetro *Hello Time* controla el intervalo de tiempo entre el envío de BPDUs de configuración. La norma 802.1d específica un valor por default de 2 segundos. Nótese

que este valor solo controla los BPDUs de configuración cuando estos son generados en el bridge Raíz, otros switches propagan BPDUs que provienen del bridge Raíz cuando son recibidos. En otras palabras, si el arrivo de BPDUs para durante un intervalo de 2 a 20 segundos debido a la turbulencia en la red, los switches que no son Bridge Raíz detienen el envío periódico de BPDUs durante este tiempo.

Forward Delay es el tiempo que el switch espera en los estados de *Listening* y *Learning*. Este es un único valor que controla ambos estados. El valor por omisión es de 15 segundos, este valor se deriva originalmente asumiendo un tamaño máximo de red de siete saltos de bridge. Con un máximo de tres BPDUs perdidos y con un intervalo de Tiempo *Hello Time* de 2 segundos. Este tiempo también se encarga de controlar el periodo de salida en la tabla de bridge después de un cambio en la topología activa.

Max Age es el tiempo que el switch guarda un BPDU antes de descartarlo. Recordando que cada puerto guarda una copia del mejor BPDU que a pasado por él. Mientras que el switch recibe continuamente BPDUs cada 2 segundos, el switch receptor mantiene una copia continua de los valores de BPDUs.

1.4.4.2 Spanning Tree por VLAN (PVST)

Es una solución para escalar y estabilizar los problemas asociados con las grandes redes Spanning Tree, crea diferentes instancias de Spanning Tree para cada VLAN.

Si se crea tolerancia a fallas en una red, un camino libre de loops debe existir entre todos los nodos de la red. El algoritmo de Spanning Tree calcula el mejor camino libre de loops a través de la red conmutada.

Debido a que cada VLAN es un segmento lógico LAN, STP mantiene una topología libre de loops en cada VLAN. Se deben habilitar solo un máximo de 64 VLANs a la vez. Si se configuran más de 64 VLANs, se pueden seguir operando las demás VLANs con el STP deshabilitado. Por omisión, STP es habilitado para las VLANs del rango 1-64.

Cada VLAN tiene una topología STP única (*root, port cost, path cost y priority*). La Figura 53 muestra que PVST mantiene instancias Spanning Tree separadas para cada VLAN, permitiendo la optimización para todas las VLANs.

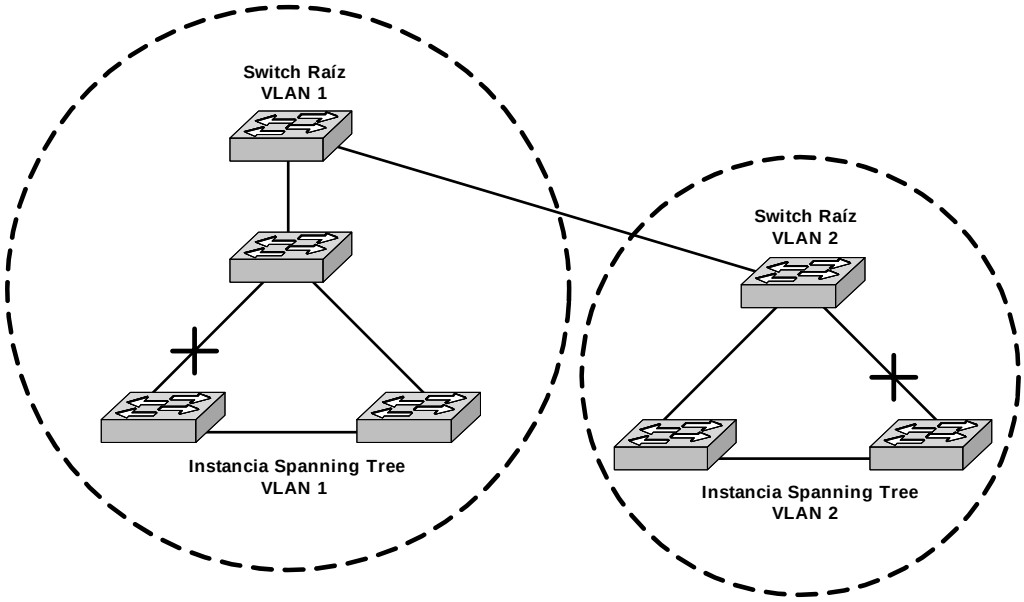


Figura 53. Diferentes instancias de Spanning Tree para cada VLAN

Si se tienen instancias separadas de Spanning Tree para cada VLAN se reducirá el tiempo de recuperación para el recalculo de STO y esto incrementa la confiabilidad de la red de las siguientes maneras:

- El tamaño total de la topología Spanning Tree se reduce
- Provee escalabilidad y se reduce el tiempo de convergencia
- Provee una rápida recuperación y una mejor confiabilidad

Las desventajas de PVST son las siguientes:

- Utilización de switches que soporten Spanning Tree por cada VLAN
- Utilización del ancho de banda del backbone para soportar los BPDUs para cada VLAN.

Como PVST trata a cada VLAN como una red por separado, este puede hacer balanceo de tráfico en capa 2, enviando el tráfico de una VLAN por un determinado enlace y el tráfico de otra VLAN por otro enlace diferente sin causar un loop de Spanning Tree.

1.4.5 Enrutadores o Routers

Un enrutador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de *Firewall* y un acceso económico a una WAN.

El enrutador opera en la capa 3 (capa de red) del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el enrutador

distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes.

El enrutador realiza dos funciones básicas:

1. Es responsable de crear y mantener las tablas de enrutamiento para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el enrutador extrae de la capa de red la dirección destino y realiza una decisión de enrutamiento basado sobre el contenido de la especificación del protocolo en la tabla de enrutamiento.

2. Permite el enrutamiento inteligente de paquetes: seleccionando la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad del enlace, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de paquetes por un enrutador puede incrementar el tiempo de espera o reducir el desempeño del enrutador cuando se compara con una simple arquitectura de switch.

Aislar el tráfico de la red, ayuda a diagnosticar problemas, puesto que cada puerto del enrutador es una subred separada, el tráfico de broadcast no pasara a través del enrutador.

Importantes beneficios del enrutador son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, FastEthernet, Token Ring, FDDI y ATM.

Otras características de los enrutadores, son:

- Muchos dominios de colisión
- Muchos dominios de broadcast

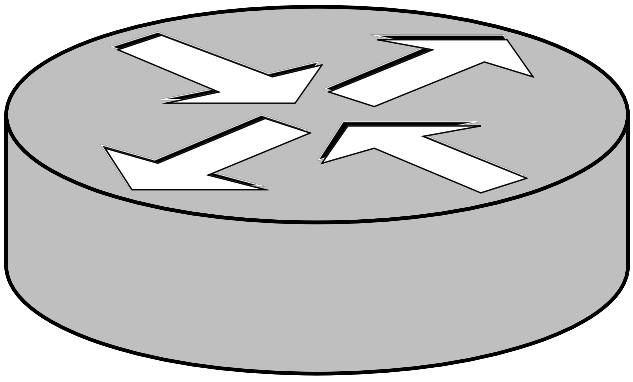


Figura 54. Diagrama Lógico de un enrutador.

1.5 TCP/IP

TCP/IP es el nombre que se le da al conjunto de protocolos que se utilizan para la comunicación a través de Internet. Fue el primer conjunto de protocolos desarrollados para ser usados en Internet. Estos protocolos se definen en base a RFCs (*Request For Comment*) que se encuentran disponibles públicamente en Internet.

En 1961, Leonard Klienrock introduce el concepto de Conmutación de Paquetes (*Packet Switching*). La idea era que la comunicación entre hosts fuera dividida en paquetes. Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red.

En 1969, la Agencia de Proyectos de Investigación Avanzada (*Defense Advanced Research Projects Agency* o DARPA) del Ejército de los EEUU desarrolla la ARPAnet. A mediados de los 70, con el desarrollo de TCP/IP empezaron, aproximadamente al mismo tiempo que se empezaban a desarrollar las redes de área local. El ejercito estadounidense gracias al proyecto ARPA (*Advanced Research Projects Agency*) invirtió muchos recursos en investigar el TCP/IP y en la interconexión de redes. Fueron unas de las primeras organizaciones que tuvo varias redes, y por lo tanto, de las primeras que se encontraron con la necesidad de tener servicios universales. La capacidad de conectar entre sí múltiples redes de manera transparente fue uno de los primeros objetivos de diseño.

Las características principales del protocolo TCP/IP son:

- Para que los hosts se puedan interconectar es necesario tener un sistema para localizar un host determinado dentro de Internet, independientemente de donde esté ubicado físicamente y de los enlaces necesarios para alcanzarlo.
- Resolver de forma automática los problemas que se puedan dar durante el intercambio de información: fallos en los enlaces, errores, pérdidas o duplicación de datos información.
- Intentar resolver las posibles incompatibilidades en la comunicación entre hosts.

En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan Intranets usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP. La siguiente tabla muestra una lista de plataformas que soportan TCP/IP:

Plataforma	Soporte de TCP/IP
UNIX	Nativo
Linux	Nativo
DOS	Piper/IP por Ipswitch
Windows	TCPMAN por Trumpet Software
Windows 95	Nativo
Windows 98	Nativo
Windows Me	Nativo
Windows XP	Nativo
Windows 2000	Nativo
Windows NT	Nativo
Macintosh	MacTCP u OpenTransport (Sys 7.5+)
OS/2	Nativo
AS/400 OS/400	Nativo

Tabla 34. Plataformas que soportan TCP/IP

Las plataformas que no soportan TCP/IP nativamente lo implementan usando programas TCP/IP de terceras partes, como puede apreciarse en la tabla anterior.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- *Aplicación:* Corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*) o SSH (Secure Shell).
- *Transporte:* Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- *Internet:* Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- *Físico:* Análogo al nivel físico del OSI.
- *Red:* Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

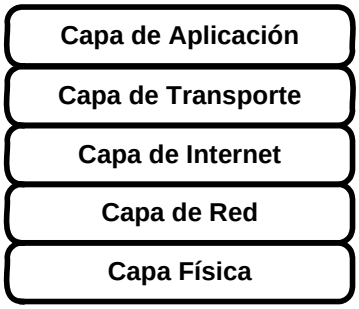


Figura 55. Arquitectura TCP/IP

1.5.1 TCP

El Protocolo de Control de Transmisión (*TCP: Transmission Control Protocol*) está pensado para ser utilizado como un protocolo host a host confiable entre miembros de redes de comunicaciones de datos por intercambio de paquetes y en un sistema interconectado de tales redes.

TCP es un protocolo orientado a la conexión, confiable entre dos extremos, diseñado para encajar en una jerarquía de capas de protocolos que soportan aplicaciones sobre múltiples redes. TCP proporciona mecanismos para la comunicación confiable entre pares de procesos en hosts ancladas en redes de comunicación de datos distintas, pero interconectadas.

TCP encaja en una arquitectura de protocolos en capas justo por encima del Protocolo de Internet, protocolo básico que proporciona a TCP, un medio para enviar y recibir segmentos de longitud variable de información envuelta en paquetes de Internet. El paquete de Internet proporciona un medio de direccionar segmentos TCP de origen y de destino situados en redes diferentes. El Protocolo de Internet también trata con la fragmentación y el reensamble de segmentos TCP que sean necesarios para conseguir el transporte y la entrega sobre múltiples redes y las puertas de enlace que las interconectan. El Protocolo de Internet también lleva información sobre la prioridad y clasificación de seguridad de los segmentos de TCP, de tal forma que esta información pueda ser comunicada de extremo a extremo entre múltiples redes.

1.5.1.1 Formato de Encabezado

Los segmentos TCP se envían como paquetes de Internet. El encabezado del protocolo de Internet transporta varios campos de información, entre los que se incluyen las direcciones de los host de origen y de destino. Un encabezado TCP sigue al encabezado de Internet, aportando información específica del protocolo TCP. Esta división permite la existencia de otros protocolos de la capa de aplicación, es decir, distintos puertos destino de TCP.

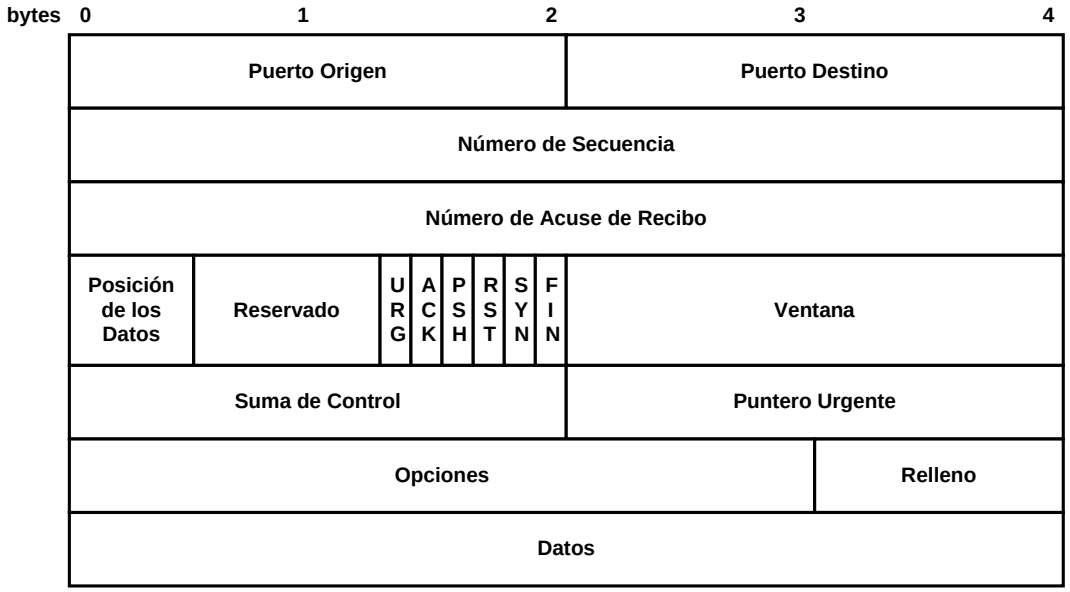


Figura 56. Formato del Encabezado TCP.

Puerto Origen (Source Port): Consta de 16 bits e indica el número del puerto origen.

Puerto Destino (Destination Port): Consta de 16 bits, indica el número del puerto destino e identifica el programa de aplicación al final de la conexión.

Número de secuencia (Sequence Number): Son 32 bits, que usualmente especifica el número asignado para el primer byte de datos en el actual mensaje. Bajo ciertas circunstancias, el campo puede ser usado para identificar el número de secuencia inicial para ser usado en una pronta transmisión.

*Número de Acuse de recibo (Acknowledgement Number**):*** Son 32 bits, que contiene el número de secuencia del siguiente byte de datos que el remitente de segmentos espera recibir.

Posición de los Datos (Data Offset): Son 4 bits, y contiene un entero que especifica la longitud del encabezado del segmento medido en múltiplos de 32 bits. Este campo es necesario porque el campo de Opciones varía en longitud dependiendo de cual de las opciones han sido incluidas. Así, el tamaño del encabezado de TCP varía dependiendo de las opciones seleccionadas.

Reservado (*Reserved):* Consta de 6 bits y esta reservado para uso futuro. Debe valer 0.

Algunos segmentos portan un acuse de recibo, mientras algunos portan datos. Otros portan peticiones para establecer o cerrar una conexión. TCP usa el campo de Bits de Control para determinar el propósito y contenido del segmento.

Bits de Control (Code Bits): 6 bits (de izquierda a derecha) para determinar :

- *URG:* Hace significativo el campo "Puntero urgente", cuando está el bit encendido.

➢*ACK:* Hace significativo el campo "Número de acuse de recibo", cuando está el bit encendido.

➢*PSH:* Función de "Entregar datos inmediatamente" ('push') , cuando está el bit encendido.

➢*RST:* Reiniciar ('Reset') la conexión, cuando está el bit encendido.

➢*SYN:* Sincronizar ('Synchronize') los números de secuencia, cuando está el bit encendido.

➢*FIN:* Últimos datos del emisor, cuando está el bit encendido.

Ventana (Window): TCP anuncia cuántos datos se aceptarán cada vez que se envía un segmento especificando el tamaño de su buffer en este campo. Son 16 bits e indican el número de octetos de datos, a contar a partir del número indicado en el campo de "Número de acuse de recibo", que el emisor de este segmento está dispuesto a aceptar.

Suma de Control (Checksuml): Son 16 bits usados para verificar la integridad de los datos en tránsito, como el encabezado TCP.

Figura 57. Seudoencabezado del Campo Suma de Control.

Puntero Urgente (Urgent Pointer): Son 16 bits. Este campo indica el valor actual del puntero urgente como un desplazamiento positivo desde el número de secuencia de este segmento. El puntero urgente apunta al número de secuencia del octeto al que seguirán los datos urgentes. Este campo es interpretado únicamente si el bit de control URG está establecido a uno.

Opciones (Options, If any): Este campo es de tamaño variable. Los campos de opciones pueden ocupar un cierto espacio al final del encabezado de TCP, pero siempre de una longitud múltiplo de 8 bits. En el cálculo de la suma de control, se incluyen todas las opciones. Una opción puede empezar en cualquier posición múltiplo de ocho.

Relleno: Es variable. El relleno del encabezado de TCP se utiliza para asegurar que el encabezado de TCP finaliza, y que los datos comienzan, en una posición múltiplo de 32 bits. El relleno está compuesto de ceros.

1.5.1.2 Características Funcionales de TCP

El propósito principal de TCP consiste en proporcionar un servicio de conexión o circuito lógico confiable y seguro entre pares de procesos. Para proporcionar este servicio encima de un entorno de Internet menos confiable, el sistema de comunicación requiere de mecanismos relacionados con las siguientes áreas:

- Transferencia básica de datos
- Confiabilidad
- Control de flujo
- Multiplexación
- Conexiones
- Prioridad y seguridad

La operación básica de TCP en cada uno de estas áreas se describe en los siguientes párrafos.

1.5.1.2.1 Transferencia Básica de Datos

TCP es capaz de transferir un flujo continuo de octetos en cada sentido entre sus usuarios, empaquetando un cierto número de octetos en segmentos para su transmisión a través del sistema de Internet. En general, los módulos de TCP deciden cuándo bloquear y enviar datos según su propia conveniencia. Algunas veces los usuarios necesitan estar seguros de que todos los datos que habían entregado al módulo de TCP han sido transmitidos. Para este propósito se define una función *push* (enviar inmediatamente). Para asegurar que los datos entregados al módulo de TCP son realmente transmitidos, el usuario emisor debe indicarlo mediante la función *push*. Un *push* en un cierto instante causa que los módulos de TCP envíen y entreguen inmediatamente al usuario receptor los datos almacenados hasta ese instante. El instante exacto en que se ejecuta la función *push* podría no ser visible para el usuario receptor. Tampoco la función *push* proporciona una marca de límite de registros.

1.5.1.2.2 Confiabilidad

El módulo de TCP debe poder recuperar los datos que se corrompan, pierdan, dupliquen o se entreguen desordenados por el sistema de comunicación del entorno de Internet. Esto se consigue asignando un número de secuencia a cada octeto transmitido, y exigiendo un acuse de recibo (ACK) del módulo de TCP receptor. Si no se recibe un ACK dentro de un cierto plazo de expiración prefijado, los datos se retransmiten. En el receptor, se utilizan los números de secuencia para ordenar correctamente los segmentos que puedan haber llegado desordenados y para eliminar los duplicados. La corrupción de datos se trata añadiendo un campo de suma de control a cada segmento transmitido, comprobándose en el receptor y descartando los segmentos dañados. En tanto, los módulos de TCP continúen funcionando adecuadamente y el sistema de Internet no llegue a quedar particionado de forma completa, los errores de transmisión no afectarán la correcta entrega de datos.

1.5.1.2.3 Control de Flujo

TCP proporciona al receptor un medio para controlar la cantidad de datos enviados por el emisor. Esto se consigue devolviendo una ventana con cada ACK, indicando el rango de números de secuencia aceptables más allá del último segmento recibido con éxito. La ventana indica el número de octetos que se permite que el emisor transmita antes de que reciba el siguiente permiso.

1.5.1.2.4 Multiplexación

Para permitir que muchos procesos dentro de un único host utilicen simultáneamente las posibilidades de comunicación de TCP, el módulo de TCP proporciona una serie de direcciones o puertos dentro de cada host. Concatenadas con las direcciones de red y de host de la capa de comunicación Internet conforman lo que se denomina una dirección de conector (*socket*). Un par de direcciones de conector identifica de forma única la conexión. Es decir, un conector puede utilizarse simultáneamente en múltiples conexiones.

La asignación de puertos a los procesos se gestiona de forma independiente en cada host. Sin embargo, resulta de máxima utilidad asignar a los procesos más utilizados frecuentemente conectores fijos que se hacen conocer de forma pública. Estos servicios pueden, entonces, ser accedidos a través de direcciones conocidas públicamente. El establecimiento y aprendizaje de las direcciones de los puertos de otros procesos puede involucrar otros mecanismos más dinámicos.

1.5.1.2.5 Conexiones

La confiabilidad y los mecanismos de control de flujo descritos anteriormente exigen que los módulos TCP inicialicen y mantengan una información de estado para cada flujo de datos. La combinación de esta información, incluyendo las direcciones de los conectores, los números de secuencia y los tamaños de las ventanas, se denomina una conexión. Cada conexión queda especificada de forma única por un par de conectores que corresponden con sus dos extremos.

Cuando dos procesos desean comunicarse, sus módulos TCP deben establecer primero una conexión (inicializar la información de estado en cada lado). Cuando la comunicación se ha completado, la conexión se termina o cierra con la intención de liberar recursos para otros usos.

Como las conexiones tienen que establecerse entre hosts no confiables y sobre un sistema de comunicación Internet no confiable, se utiliza un mecanismo de acuerdo al uso de números de secuencia, basados en tiempos de reloj para evitar una inicialización errónea de las conexiones.

1.5.1.2.6 Prioridad y Seguridad

Los usuarios TCP pueden indicar el nivel de seguridad y prioridad de su comunicación. Se emplean valores por defecto cuando estas características no se necesiten.

1.5.2 IP

IP (*Internet Protocol*) está diseñado para su uso en sistemas interconectados de redes de comunicación de hosts por intercambio de paquetes. IP proporciona los medios necesarios para la transmisión de bloques de datos llamados paquetes desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. IP también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes paquetes para su transmisión a través de las redes.

IP está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits desde un origen a un destino a través de un sistema de redes interconectadas. No existen mecanismos para aumentar la confiabilidad de datos entre los extremos, control de flujo, secuencia u otros servicios que se encuentran normalmente en otros protocolos host a host. IP puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

IP implanta dos funciones básicas: direccionamiento y fragmentación.

- Las redes usan las direcciones que se encuentran en el encabezado IP para transmitir los paquetes IP hacia sus destinos. La selección de un camino para la transmisión se llama enrutamiento.
- Las redes usan campos en el encabezado IP para fragmentar y reensamblar los paquetes IP cuando sea necesario para su transmisión a través estas.

El modelo de operación es que un módulo IP reside en cada host involucrado en la comunicación y en cada enrutador que interconecta las redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar paquetes IP. Además, estos módulos (especialmente en los enrutadores) tienen procedimientos para tomar decisiones de enrutamiento y otras funciones.

IP trata cada paquete como una entidad independiente no relacionada con ningún otro paquete. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo).

IP utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de encabezado.

- El Tipo de Servicio (*Type of Service*) se utiliza para indicar la calidad de servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes. Esta indicación de tipo de servicio será usada por los enrutadores para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o el siguiente enrutador al enrutar un paquete.
- El Tiempo de Vida (*Time to Live*) es una indicación de un límite superior en el periodo de vida de un paquete. Es fijado por el remitente del paquete y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el paquete llegue a su destino, el paquete es descartado.
- Las Opciones *(Options)* proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y enrutamiento especial.
- La Suma de Control del Encabezado (*Checksum*) proporciona una verificación de que la información utilizada al procesar el paquete, ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control del encabezado falla, el paquete es descartado inmediatamente por la entidad que detecta el error.

IP no proporciona ningún mecanismo de comunicación confiable. No existen acuses de recibo, ni entre extremos, ni entre saltos. No hay control de errores para los datos, sólo una suma de control del encabezado. No hay retransmisiones. No existe control de flujo.

Los errores detectados pueden ser notificados por medio del Protocolo de Mensajes de Control de Internet (*ICMP: Internet Control Message Protocol*) el cual está implantado en el módulo IP.

1.5.2.1 Características Funcionales de IP

La función o propósito de IP es mover paquetes a través de un conjunto de redes interconectadas. Esto se consigue pasando los paquetes desde una red a otra hasta que se alcanza el destino. Los módulos IP residen en hosts y enrutadores. Los paquetes son enrutados desde un módulo IP a otro a través de redes individuales basándose en la interpretación de una dirección IP. Por eso, un mecanismo importante de IP es la dirección lógica o dirección IP.

En el enrutamiento de paquetes de una red a otra, los paquetes pueden necesitar atravesar una red con diferentes tamaños de Unidades de Transferencia Máxima (*MTU: Maximum Transmission Unit*) cuyo tamaño máximo de paquete es menor que el tamaño del paquete. Para evitar este problema se proporciona un mecanismo de fragmentación y reensamblaje de paquetes.

1.5.2.1.1 Direccionamiento

Se establece una distinción entre nombres, direcciones y rutas. Un nombre indica qué buscamos. Una dirección indica dónde está. Una ruta indica cómo llegar allí. IP maneja direcciones lógicas. Es tarea de los protocolos de niveles mayores, es decir, protocolos host a host o entre aplicaciones hacer corresponder nombres con direcciones. IP hace corresponder direcciones de IP con direcciones de red local. Es tarea de los procedimientos de menor nivel, es decir, redes locales o enrutadores realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de una longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección de host. Hay 3 formatos o clases de direcciones IP: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección de host; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección de host; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección de host.

Se debe tener cuidado al relacionar direcciones de red con direcciones de host; un host individual físicamente hablando debe ser capaz de actuar como si fuera varios hosts distintos, hasta el punto de usar varias direcciones IP distintas. Algunos hosts tendrán también varios interfaces físicas (*multihoming*).

Esto quiere decir que se debe establecer algún mecanismo que permita a un host tener varios interfaces físicas de red, cada uno de ellas con varias direcciones lógicas IP.

1.5.2.1.2 Fragmentación

La fragmentación de un paquete es necesaria cuando éste se origina en una red local que permite un tamaño de paquete grande, es decir, el tamaño de MTU y debe atravesar una red local que limita los paquetes a un tamaño inferior para llegar a su destino.

Un paquete puede ser marcado como "no fragmentar". Todo paquete así marcado no será fragmentado entre distintas redes bajo ninguna circunstancia. Si un paquete marcado como "no fragmentar" no puede ser entregado en su destino sin fragmentarlo, entonces debe ser descartado.

La fragmentación, transmisión y reensamblaje a través de una red local invisible para IP se llama fragmentación Intranet y puede ser utilizada.

El procedimiento de fragmentación y reensamblaje en IP tiene que ser capaz de dividir un paquete en un número casi arbitrario de piezas que puedan ser luego reensambladas. El receptor de los fragmentos utiliza el campo de identificación para asegurarse de que no se mezclan fragmentos de distintos paquetes. El campo posición (*offset*) le indica al receptor la posición de un fragmento en el paquete original. La posición y longitud del fragmento determinan la porción del paquete original comprendida en este fragmento. El indicador más-fragmentos (*more fragment*) indica, puesto a cero, el último fragmento. Estos campos proporcionan información suficiente para reensamblar el paquete.

Para fragmentar un paquete IP grande, un módulo IP, por ejemplo, un enrutador crea dos nuevos paquetes y copia el contenido de los campos del encabezado IP del paquete grande en los dos encabezados nuevos. Los datos del paquete original son divididos en dos fragmentos tomando una resolución mínima de 8 octetos (64 bits), el segundo fragmento puede no ser un múltiplo entero de 8 octetos, pero el primero sí debe serlo. Llamemos al número de bloques de 8 octetos en el primer fragmento Número de Bloques del Fragmento (*NFB: Number of Fragment Blocks*). El primer fragmento de datos es colocado en el primer nuevo paquete y el campo longitud total se establece a la longitud del primer paquete. El indicador “más fragmentos" es puesto a uno. El segundo fragmento de datos es colocado en el segundo nuevo paquete y el campo longitud total se establece a la longitud del segundo paquete. El indicador "más fragmentos" lleva el mismo valor que en el paquete original. El campo posición del segundo nuevo paquete se establece al valor de ese campo en el paquete original más el NFB.

Este procedimiento puede generalizarse para una n-partición, mejor que para la división en dos partes descrita.

Para ensamblar los fragmentos de un paquete, IP, por ejemplo, en un host destino, combina todos los paquetes que tengan el mismo valor en los cuatro campos: identificación, origen, destino y protocolo. La combinación se realiza colocando el fragmento de datos de cada fragmento en su posición relativa indicada por la posición del fragmento en el encabezado IP de ese fragmento. El primer fragmento tendrá posición cero, y el último fragmento tendrá el indicador "más fragmentos" puesto a cero.

1.5.2.2 Formato de Encabezado IP

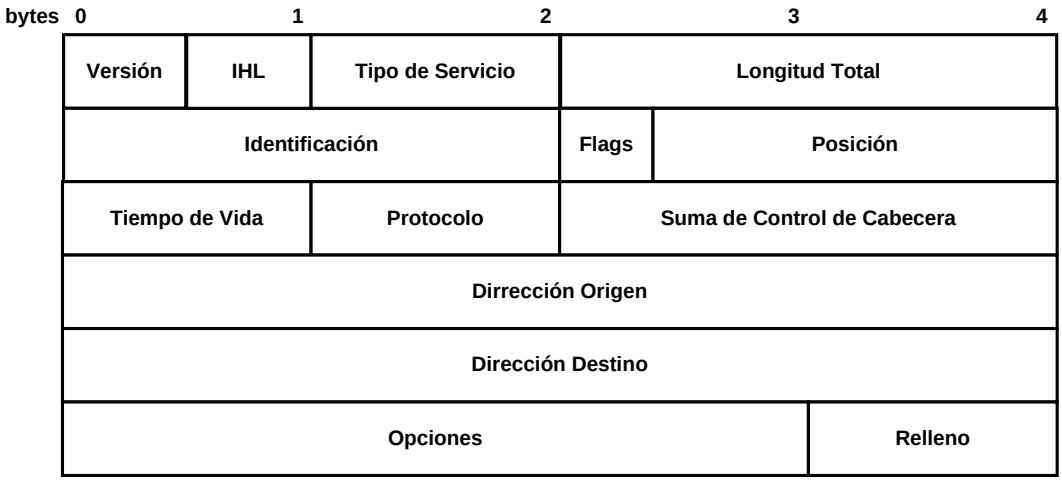


Figura 58. Formato de Encabezado IP

Versión (Version): Consta de 4 bits. El campo versión describe el formato del encabezado IP.

IHL: Son 4 bits. Longitud del Encabezado Internet (Internet Header Length), es la longitud del encabezado en palabras de 32 bits, y por tanto, apunta al comienzo de los datos. El valor mínimo para un encabezado correcto es 5.

Tipo de Servicio (Type of Service): Consta de 8 bits. El tipo de servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseado. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir en un paquete a través de una red en particular. Algunas redes ofrecen prioridad de servicio, la cual trata de algún modo el tráfico de alta prioridad como más importante que el resto del tráfico (generalmente aceptando sólo tráfico por encima de cierta prioridad en momentos de sobrecarga). La elección más común es un compromiso a tres niveles entre baja demora, alta confiabilidad, y alto rendimiento.

Bits 0-2: Prioridad.
Bit 3: 0 = Demora Normal, 1 = Baja Demora.
Bit 4: 0 = Rendimiento Normal , 1 = Alto rendimiento.
Bit 5: 0 = Confiabilidad Normal , 1 = Alta Confiabilidad.
Bits 6-7: Reservado para uso futuro.

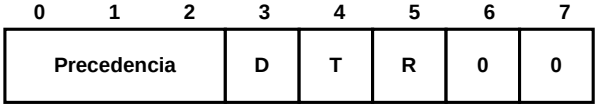


Figura 59. Formato del Campo Tipo de Servicio

Precedencia

111 - Control de Red
110 - Control Entre Redes
101 - CRITICO/ECP
100 - Muy urgente (Flash Override)
011 - Urgente (Flash)
010 - Inmediato
001 - Prioridad
000 - Rutina

El uso de las indicaciones de retraso, rendimiento y confiabilidad puede incrementar el costo, en cierto sentido, del servicio. En muchas redes un mejor rendimiento para uno de estos parámetros conlleva un peor rendimiento en algún otro. Excepto para casos excepcionales no se deben establecer más de dos de estos tres indicadores.

El tipo de servicio se usa para especificar el tratamiento del paquete durante su transmisión a través de la red. Se dan ejemplos de relación entre el tipo de servicio IP y el servicio real proporcionado por redes como AUTODIN II, ARPANET, SATNET y PRNET en "Correspondencias de Servicios"´.

La denominación de precedencia 'Control de Red' está pensada para ser usada dentro de una sola red. El uso y control efectivos de este modo es responsabilidad de cada red. El modo 'Control Entre Redes' está pensado para su uso exclusivo por parte de generadores de control de enrutadores. Si el uso efectivo de estos modos de precedencia concierne a una red en particular, es responsabilidad de esa red controlar el acceso a, y el uso de, esos modos de precedencia.

Longitud Total (Total Length): Este campo es de 16 bits. La longitud total es la longitud del paquete, medida en octetos, incluyendo el encabezado y los datos. Este campo permite que la longitud máxima de un paquete ser de 65,535 octetos. Los paquetes de tal longitud no son prácticos para la mayoría de hosts y redes. Todos los hosts deben estar preparados para aceptar paquetes de hasta 576 octetos, tanto si llegan completos como en fragmentos. Se recomienda que los hosts envíen paquetes mayores de 576 octetos sólo si tienen la seguridad de que el destinatario está preparado para aceptarlos.

El número 576 se ha seleccionado para permitir que un bloque de datos de tamaño razonable sea transmitido junto a la información del encabezado necesario. Por ejemplo, este tamaño permite que un bloque de datos de 512 octetos más 64 octetos de encabezado quepa en un paquete. El encabezado IP de tamaño máximo son 60 octetos, y un encabezado IP típico son 20 octetos, admitiendo así un margen para encabezados de protocolos de nivel superior.

Identificación (Identification): Consta de 16 bits y es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un paquete.

Banderas (Flags): Son 3 bits y son diversos indicadores de control.

Bit 0: reservado, debe ser cero.
Bit 1: (DF) No Fragmentar (*Don't Fragment*) 0 = puede fragmentarse,
1 = No Fragmentar.

Bit 2: (MF) Más Fragmentos (*More Fragments*) 0 = Último Fragmento,
1 = Más Fragmentos.

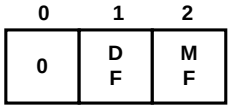


Figura 60. Formato del Campo Flags

Posición del Fragmento (Fragment Offset): Consta de 13 bits. Este campo indica a que parte del paquete pertenece este fragmento. La posición del fragmento se mide en unidades de 8 octetos (64 bits). El primer fragmento tiene posición 0.

Tiempo de Vida (Time to Live): Son 8 bits. Este campo indica el tiempo máximo que el paquete tiene permitido permanecer en la red. Si este campo contiene el valor cero, entonces el paquete es descartado. Este campo es modificado durante el procesamiento del encabezado IP. El tiempo es medido en segundos, pero como todo dispositivo que procese un paquete debe decrementar el Timpo de Vida al menos en uno, incluso si procesa el paquete en menos de un segundo o en más, se debe pensar en el TTL sólo como un límite superior del tiempo durante el cual un paquete puede existir, es decir, es leído por número de saltos. La intención es hacer que los paquetes imposibles de entregar sean descartados, y limitar el máximo periodo de vida de un paquete.

Protocolo (Protocol): Este campo consta de 8 bits. Indica el protocolo del siguiente nivel usado en la parte de datos del paquete IP. Los valores de varios protocolos son especificados en "Números Asignados".

Suma de Control del Encabezado (Header Checksum): Son 16 bits. Suma de Control del encabezado solamente. Dado que algunos campos del encabezado cambian, por ejemplo, el tiempo de vida, esta suma es recalculada y verificada en cada punto donde el encabezado es procesado.

El algoritmo de la suma de control es*:* el campo suma de control es el complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits del encabezado. A la hora de calcular la suma de control, el valor inicial de este campo es cero.

Esta es una suma de control fácil de calcular y la evidencia experimental indica que es adecuada, pero es provisional y puede ser reemplazada por un procedimiento CRC, dependiendo de la experiencia anterior.

Dirección Origen (Source Address): Este campo es de 32 bits. Es la dirección IP origen.

Dirección Destino (Destination Address): Consta de 32 bits. Es la dirección IP destino.

Opciones (Options): Este campo es de longitud variable. Las opciones pueden o no aparecer en los paquetes. Deben ser implementadas por todos los host y enrutadores. Lo que es opcional es su transmisión en cualquier paquete en particular, no su implantación.

Valor de Relleno (+Padding): Es de tamaño variable. El Valor de Relleno se usa para asegurar que el encabezado IP ocupa un múltiplo de 32 bits. El valor de relleno es cero.

1.5.3 Direccionamiento IP

Para proporcionar flexibilidad en la asignación de direcciones a redes y tener en cuenta un gran número de redes de pequeño a medio tamaño, la interpretación del campo dirección está codificada para especificar un pequeño número de redes con un gran número de hosts, un número moderado de redes con un número moderado de hosts, y un gran número de redes con un pequeño número de hosts.

El protocolo IP identifica a cada host que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada host, y se representa como cuatro cifras de 8 bits separadas por puntos.

La dirección de Internet se utiliza para identificar tanto al host en concreto como la red a la que pertenece, de manera que sea posible distinguir a los hosts que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de hosts en cada una de las redes de esta clase.

Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 hosts en la misma red.

Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 host en cada red.

Clase D. Las direcciones de clase D se reservan para multicasting o multidifusión, usadas para direccionar grupos de hosts en un área limitada.

Clase E. Las direcciones de clase E se reservan para usos en el futuro.

Mascara de red. La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. Es usada para agrupar direcciones IP. Por ejemplo, una subred 192.168.0.0 con la máscara

255.255.255.0, las direcciones que podremos asignarles a los hosts en la subred irán de 192.268.0.1 hasta 192.168.0.254. Cada dirección IP consiste de dos partes (la dirección de red y el número de máquina). La máscara de red se usa para determinar el tamaño de cada una de estas partes. Las posiciones de los bits en uno de la máscara se consideran parte del espacio reservado para la dirección de red, mientras que los bits que están puestos a cero se consideran parte del espacio apartado para el número de host. En formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha.

Para comprobar si un host pertenece a una red, tendremos que convertir su Dirección IP a sistema binario y hacer un AND bit a bit sobre la máscara de red si el resultado es la dirección de la red pertenece a la red de lo contrario no pertenece.

Queremos comprobar si tres hosts con las siguientes direcciones IP pertenecen a la misma red.

10.128.180.25
10.128.181.36
10.128.182.44

Y la máscara de red es 255.255.254.0

Realizamos la comprobación
Dirección IP - IP en Binario
10.128.180.25 - 00001010.10000000.10110100.00011001
255.255.254.0 - 11111111.11111111.11111110.00000000
Resultado ------ 00001010.10000000.10110100.00000000
10.128.180.0 (Pertenece a la Red)

Dirección IP - IP en Binario
10.128.181.36 - 00001010.10000000.10110101.00100100
255.255.254.0 - 11111111.11111111.11111110.00000000
Resultado ------ 00001010.10000000.10110100.00000000
10.128.180.0 (Pertenece a la red)

Dirección IP - IP en Binario
10.128.182.44 - 00001010.10000000.10110110.00101100
255.255.254.0 - 11111111.11111111.11111110.00000000
Resultado ------ 00001010.10000000.10110110.00000000
10.128.182.0 (No pertenece a la red)

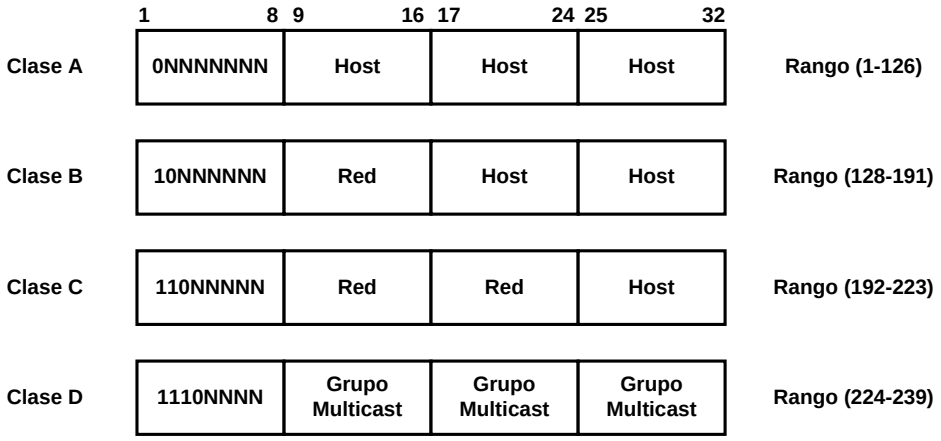


Figura 61. Clases de Direcciones IP

Las redes 127.0.0.0, 10.0.0.0, 172.16.0.0 hasta la 172.31.0.0 y la 192.168.0.0 son redes reservadas y no son usadas en la red pública. La red 127.0.0.0 es la red que tiene su origen y fin en el host propio, es utilizada para pruebas; la dirección 127.0.0.1 es la dirección de retorno, *loopback* o *localhost* y se reserva para el tráfico local del propio nodo, apunta al host propio, se utiliza para probar el funcionamiento y los servicios de red sin estar conectado a ningún tipo de red.

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	Máscara de subred
A	r.h.h.h	128	16777214	1.0.0.0 – 126.0.0.0	255.0.0.0
B	r.r.h.h	16384	65534	128.0.0.0 – 191.255.0.0	255.255.0.0
C	r.r.r.h	2097152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	no válidas	-	-	240.0.0.0 - 255.255.255.255	-

Tabla 35. Las direcciones IP

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de host para máquinas que aún no conocen su número de host dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los hosts conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo paquete a un número determinado de hosts, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un host a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible. Internet y en las líneas punto a punto no es posible enviar broadcast, pero sí que es posible hacerlo en las redes Ethernet, donde se supone que todos los hosts prestarán atención a este tipo de mensajes.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (*subnets*). Como ejemplo, podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bytes. En este caso sería posible utilizar el tercer byte para indicar en qué red Ethernet se encuentra un host en concreto. Esta división no tendrá ningún significado para cualquier otro host que esté conectado a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

Las direcciones IP se clasifican en:

Direcciones IP públicas. Son visibles en todo Internet. Un host con una IP pública es accesible (visible) desde cualquier otro host conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por enrutadores. Se utilizan en las empresas para los puestos de trabajo. Los hosts con direcciones IP privadas pueden salir a Internet por medio de un enrutador (o *proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas. Las direcciones privadas son usadas para la configuración de nuestra red internamente. El RFC 1918 define el rango de direcciones que debemos de usar en nuestra red privada:

- Clase A: 10.0.0.0 - 10.255.255.255 equivalente a una red de clase A (prefijo 10/8),
- Clase B: 172.16.0.0 - 172.31.255.255 equivalente a 16 redes de clase B (prefijo 172.16/12),
- Clase C: 192.168.0.0 - 192.168.255.255 equivalente a 256 redes de clase C (prefijo 192.168/16).

A su vez, las direcciones IP pueden ser:

Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Servicio de Internet (ISP, Internet Service Provider) utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP, es poco probable que todos se conecten a la vez.

Las IP dinámicas se pueden asignar mediante los siguientes protocolos:

1. Protocolo de Resolución inversa de Direcciones *(RARP: Reverse Ardes Resolution Protocol):* Permite que un host que acaba de arrancar o sin disco pueda encontrar su dirección IP desde un servidor. Para ello utiliza el direccionamiento físico de red, proporcionando la dirección MAC de la máquina de destino para identificar de manera única el procesador, transmitiendo por broadcast la solicitud RARP. Una vez que el host obtiene su dirección IP la guarda en memoria, y no vuelve a usar RARP hasta que no se inicia de nuevo.

2. BOOTP *(Bootstrap Protocol).* En los años 80 era habitual utilizar un protocolo muy sencillo llamado BOOTP que permitía que algunos sistemas (normalmente máquinas Unix corriendo /etc/bootpd) asignaran direcciones IP a sistemas tales como impresoras o servidores de terminales. El servidor utilizaba un sencillo fichero de texto para buscar la dirección MAC del "cliente" y le asignaba la dirección IP (y algún otro parámetro) según constara en dicho fichero. Actualmente este sistema se usa, por ejemplo, para algunos elementos de electrónica de red como switches o concentradores y en ciertos modelos de impresoras con interfaz de red local. El protocolo BOOTP utilizaba una estructura de tramas muy sencilla y el tráfico generado era mínimo. Desgraciadamente, no es suficiente para la mayoría de los casos y en redes de tamaño medio, su eficacia es muy baja. BOOTP funciona sobre un datagrama UDP encapsulado sobre IP, este paquete se envía a la dirección de broadcast, el servidor de BOOTP recibe ese paquete y devuelve a la dirección de broadcast la respuesta, el host origen cuando ve en el paquete de broadcast su dirección MAC lo recoge y ya sabe cual es su dirección IP, BOOTP puede enviar no solo la dirección del host, si no también la dirección de la puerta de enlace y la del servidor BOOTP. Con BOOPT se puede crear un fichero con las características de cada uno de los hosts, ya que no fue diseñado para direccionamiento dinámico en sus origenes.

3. DHCP. A principios de la década de los 90, la IETF desarrolló el protocolo DHCP (*Dynamic Host Configuration Protocol*). Su objetivo principal era superar las posibilidades de BOOTP, ampliándolo y permitiendo que los administradores de redes se olvidaran, casi por completo, de la asignación de direcciones IP a las decenas o centenares de hosts y otras máquinas de su organización. DHCP se basa en el conocido modelo Cliente-Servidor. Utiliza un protocolo de comunicaciones muy sencillo (basado en UDP sobre IP). Los clientes de una red

que utilicen este protocolo utilizan direcciones IP que les "alquila" un servidor (no tiene porqué ser local). Cada vez que un cliente se inicia, pide una dirección IP o una renovación de la que tiene alquilada actualmente. El cliente recibe, junto con la dirección, algunos parámetros adicionales: enrutador por defecto, servidor WINS, servidor DNS, etc. La intervención del administrador de redes, aún en grandes configuraciones es mínima. A diferencia de BOOTP, DHCP permite asignar y liberar las direcciones IP de forma rápida y dinámica de forma automática, evitando las duplicidades y se optimiza el consumo de direcciones. Lo único que necesita es un *pool* de direcciones libres para asignar, de esta, manera DHCP va asignando direcciones de forma dinámica de ese rango que tiene para asignar. La estación envía un paquetes de broadcast de datagramas UDP, con el puerto BOOTP (DHCPDISCOVER), el host pasa a estado SELECCIÓN y recibe las respuestas del servidor de DHCP llamadas DHCPOFFER, una vez recibida la respuesta negocia el tiempo que puede tener esa IP sin renegociarla con un paquete DHCPREQUEST, después el servidor confirma la petición del host con un DHCPACK, en este momento el host ya puede empezar a trabajar.

1.5.3.1 Subnetting

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podían ser necesarios cuando:

- Se instala una nueva red física.
- Desperdicio de direcciones.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.

Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de subred. El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina subred. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como

<número de red<número de subred<número de host

La combinación del número de subred y del host suele denominarse dirección local o parte local. La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de una red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a 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 una máscara de subred que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a uno pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de "todos los bits a cero" y "todos los bits a uno" se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254 (256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.

- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4094 posibles subredes (4096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay otras posibilidades.

Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un número de bits al número de subred y el resto a la dirección local. Por tanto, es común usar un bloque de bits contiguos al comienzo de la parte local para el número de subred ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

1.5.3.2 VLSM: Variable Length Subnet Masks

El RFC 1009 redactado en 1987 especifica como una red que utiliza subneteo puede usar más de una máscara de subred. Cuando a una Red IP se le asigna mas de una máscara de subred, esta es considerada una red que esta utilizando mascaras de subred de longitud variable (VLSM) por que las mascaras de subred tienen diferentes longitudes.

El uso de mascaras múltiples de subred permite el uso más eficiente para la asignación de direcciones IP. También ayuda a reducir significativamente la gran información de enrutamiento para el nivel backbone en el dominio de enrutamiento de las organizaciones.

VLSM soporta el uso más eficiente del espacio de direcciones IP asignadas de las organizaciones. Uno de los mayores problemas con la temprana limitación de solo soportar una mascara de subred a través de un número de red dado es que solo una mascara fue seleccionada, esto bloquea a la organización en un número dado de subredes limitadas ya en tamaño. Por ejemplo, en el caso que un administrador decide configurar la red 130.5.0.0/16 con un máscara de subred de /22.

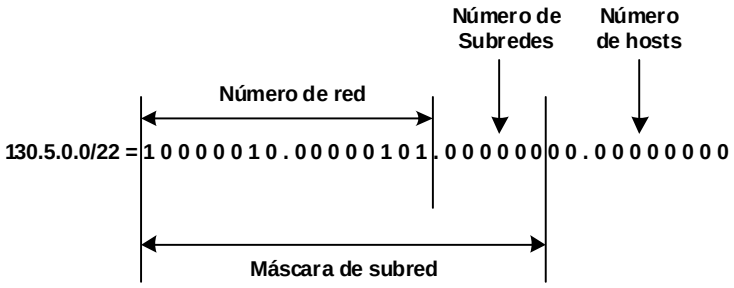


Figura 62. La red 130.5.0.0/16 con una máscara de subred de 22 bits.

En la figura anterior tenemos una red con mascara de red de 16 bits y con una mascara de subred de 22 bits, cada una de las cuales soporta un máximo de 1,022 hosts (2^{10} - 2). Esto esta bien si la organización quiere trabajar con un número de subredes grandes, pero que tal si se tiene que alguna de sus subredes es pequeña y solo contiene alrededor de 20 o 30 hosts. Desde que una red en la cual se ha utilizado subneteo tiene solo una máscara de sudred, el administrador de red tendrá que asignar la subred de 20 o 30 hosts a una subred con un prefijo de 22 bits. En esta asignación se desperdiciarían alrededor de 1,000 direcciones IP por cada subred pequeña configurada.

Una solución para este problema fue permitir la asignación de más de una mascara de subred en una red en la cual se realiza subneteo. En relación con el ejemplo anterior, si al administrador de red se le da la misma red, 130.5.0.0/16 con una mascara de subred de 22 bits: ahora tendría 1024 subredes (2^{10}) con una capacidad de 62 hosts cada una (2^6 - 2). El prefijo de 26 bits es ideal para pequeñas subredes con menos de 60 hosts, mientras que el prefijo de 22 bits es bueno para subredes grandes que contengan más de 1000 hosts.

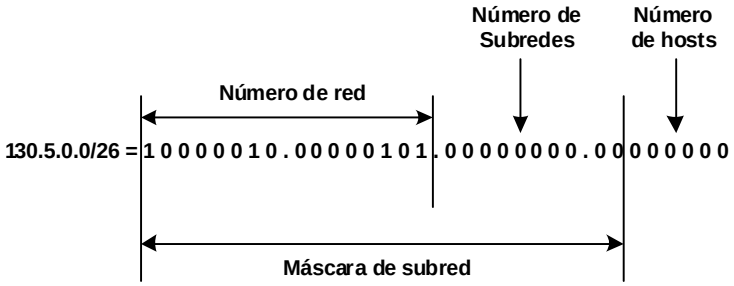


Figura 63. La red 130.0.0.0/16 con una mascara de subred de 26 bits.

VLSM también permite la división recursiva de el espacio de direcciones en la organización esto puede ser reensamblado y agregado para reducir la gran cantidad de información de enrutamiento en el nivel más alto. Conceptualmente, una red es primero dividida en subredes, algunas de esas subredes son posteriormente divididas en otras subredes, y algunas de estas son divididas en otras subredes más pequeñas. Esto trae consigo que la detallada estructura detallada de la información de enrutamiento para un grupo de alguna subred sea escondida por los enrutadores de otro grupo de subred.

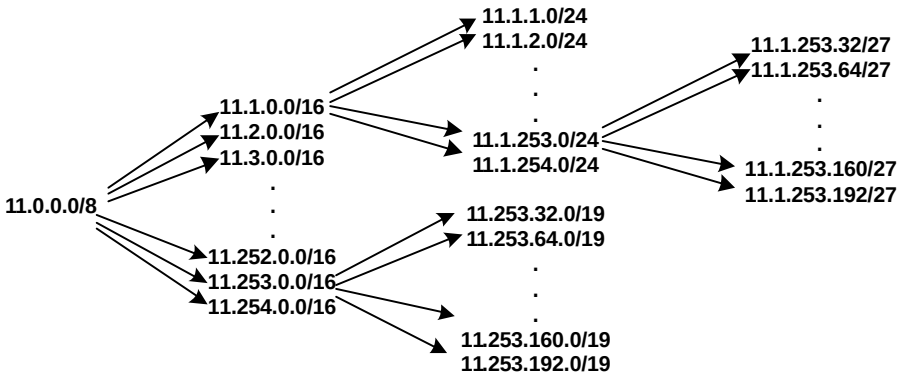


Figura 64. VLSM permite la división recursiva del número de red

En la figura 64, la red 11.0.0.0/8 es primero configurada con una máscara de subred de 16 bits, posteriormente la subred 11.0.0.0/16 es configurada con una máscara de subred de 24 bits y la subred 11.253.0.0/16 es configurada con una máscara de subred de 19 bits. Nótese que el proceso recursivo no requiere que la misma máscara de subred sea signada en cada uno de los niveles de recursividad. También, la recursiva subdivisión del espacio de direcciones puede ser utilizada de acuerdo a la necesidad del administrador de red para la asignación de nuevas subredes.

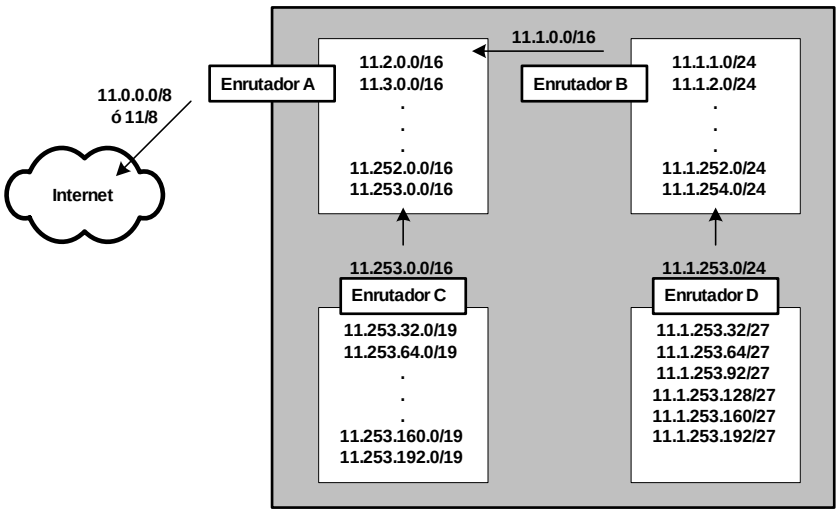


Figura 65. VLSM permite la reducción del tamaño de la tabla de enrutamiento mediante la agregación de rutas

La figura 65, ilustra como una buena planeación y utilización de VLSM trae consigo la reducción del tamaño de las tablas de enrutamiento. Notando que el enrutador D esta habilitado para agregar a las seis subredes detrás de las cuales solo existe una única dirección anunciada (11.1.253.0/24) y como el enrutador B es habilitado para agregar a todas las subredes que están detrás de él a partir de una sola dirección anunciada. De igual manera el enrutador C es habilitado para sumarizar a las seis subredes que están detrás de la única dirección anunciada (11.253.0.0/16). Finalmente, se puede notar que a pesar de que la estructura de las subredes no es visible hacia fuera de la organización el

enrutador A posee una sola ruta en la tabla global de enrutamiento de Internet, 11.0.0.0/8 (ó 11/8).

1.5.3.3 CIDR: Clasless Inter-Domain Routing. Classless Addressing (Supernetting)

El subneteo fue inventado al inicio de los años 80s para ayudar a conservar el espacio de direcciones IP; surgiendo una nueva técnica para direccionar redes. En 1993, se pensó aparentemente que este tipo de técnicas por si solas no iban a prevenir el crecimiento de Internet y el uso exhaustivo del espacio de direcciones IP. Pero gracias al trabajo se logro una nueva versión de IP que ayudarían a mejorar el aprovechamiento de las direcciones IP. Para solucionar el problema del crecimiento hasta que la nueva versión de IP fuera normalizada y adoptada, se encontró una solución temporal.

Esta solución llamada *classless adresing*, *supernet addressing* o *supernetting*, es una aproximación que complementa el direccionamiento para las subredes. En lugar de solo usar un único prefijo IP de red para múltiples redes físicas en una organización, supernetting permite a las direcciones asignadas a una sola organización tomar un sin numero de prefijos clasificados.

Para entender por que el direccionamiento classless fue adoptado, se necesita conocer los tres factores que se consideraron. El primero fue que el esquema classful no divide las direcciones de red en clases iguales en número. A pesar de que menos de 17000 redes clase B pueden ser asignadas, existen más de 2 millones de redes C. El segundo factor indica que las redes clase C han sido requeridas muy lentamente, ya que solo se han asignado un porcentaje pequeño de ellas. Y por último, los estudios muestran que a la razón que los números de red clase B están siendo asignados, los prefijos de clase B podrían acabarse rápidamente. Esta Situación se convirtió en el problema conocido como *Running Out of Ardes Space* (ROADS).

Para comprender como trabaja el supernetting, considerando una organización de tamaño mediano que tiene salida hacia le red Internet. Dado que una organización prefiere usar un solo conjunto de direcciones de clase B debido a dos cuestiones: una red clase C no pueden direccionar más de 254 host y una clase B tiene los bits suficientes para utilizar subnetting de manera efectiva. Para conservar los números de clase B, el esquema de supernetting asigna a la organización un conjuntote clases C en vez de una sola clase B. Por ejemplo, consideremos que una organización requiere de una solo clase B e intenta hacer subnetting con el tercer octeto utilizándolo como su número de subred. En vez de utilizar una sola Clase B, supernetting asigna a la organización un conjunto de 256 clases C contiguas que la organización puede asignar a sus redes físicas.

Aunque el supernetting es fácil de entender cuando se ve como una manera de satisfacer a una sola organización, el supernetting intento ser utilizado en otro contexto. Algunos vieron la posibilidad de un Internet Jerárquico donde los Proveedores de Servicios de Internet (ISP) abastecieran la conectividad a Internet. Para conectar sus redes a Internet, las organizaciones contratan a un ISP, el proveedor del servicio controla la designación de direcciones IP para la organización, así como la instalación de las conexiones físicas. Los diseñadores de supernetting plantearon que los ISPs podrían asignar un gran número de

direcciones, debido a que pueden dar una o mas direcciones a cada uno de sus suscriptores o clientes.

1.5.1.3.1 El efecto del Supernetting en el Enrutamiento

Asignando muchas clases C en vez de una sola clase B, se conservan las clases B y resuelves el problema de agotamiento del espacio de direcciones. Sin embargo, esto crea un nuevo problema: la información que los enrutadores guardan e intercambian se incrementa dramáticamente. Por ejemplo, asignando a una organización 256 clases C en vez de una clase B se requiere de 256 enrutadores en vez de 1.

La técnica conocida como *Classless Inter-Domain Routing* (CIDR) resuelve el problema. Conceptualmente, CIDR colapsa a un grupo contiguo de clases C en una sola entrada representada por:

(número de red, contador)

Donde el número de red es la dirección más pequeña en el grupo y el contador indica el número total de redes en el grupo. Por ejemplo, (192.5.48.0,3) es usado para indicar las siguientes tres redes: 192.5.48.0, 192.5.49.0 y la 192.5.50.0.

Si un grupo pequeño de ISPs forman el núcleo de Internet y cada uno posee un gran conjunto de direcciones IP de red contiguas, el beneficio de usar supernetting se puede ver con facilidad: las tablas de enrutamiento son mucho más pequeñas. Si consideramos las entradas en la tabla de enrutamiento de los enrutadores del proveedor de Internet. La tabla debe contener la ruta correcta para cada suscriptor, pero la tabla no necesita contener los enrutadores de los demás ISPs. En lugar de eso, la tabla guarda solo una entrada para cada uno de los otros proveedores, esta entrada identifica el grupo de direcciones que le pertenecen a cada proveedor.

1.5.1.3.2 Grupo de Direcciones CIDR y Mascaras de Bits

En la práctica, CIDR no restringe los números de red solo a clases C y no los usa como un valor entero para especificar el tamaño de un grupo. En lugar de eso, CIDR requiere el tamaño de cada grupo de direcciones, y usa una mascara de bits para identificar el tamaño del grupo. Por ejemplo, si a una organización se le asigna un bloque de 2048 direcciones contiguas comenzando por la dirección 128.211.168.0., la Tabla 36 muestra los valores binarios para el rango de las direcciones.

	Formato Decimal	**Formato de 32 Bits**
Dirección más baja	128.211.168.0	10000000 11010011 10101000 00000000
Dirección más alta	128.211.175.255	10000000 11010011 10101111 11111111

Tabla 36. Ejemplo de un bloque de 2048 direcciones CIDR. Esta tabla muestra las direcciones mínima y máxima del rango en formato decimal y binario.

CIDR necesita dos elementos para especificar un bloque de direcciones: el valor de 32 bits de la dirección más bajo en el bloque de direcciones y una máscara de 32 bits. La máscara opera como una máscara de subred estándar, delineando el fin del prefijo. Para el rango mostrado, una máscara CIDR de 21 bits ha sido preparada, lo cual significa que la división entre el prefijo y el sufijo ocurre después del bit con posición número 21.

11111111 11111111 11111000 00000000

1.5.3.3.3 Bloque de Direcciones y la Notación CIDR

Dado que un bloque de direcciones CIDR necesita de una dirección y de una máscara, se invento una notación que considerara estos dos elementos. Llamada notación CIDR pero conocida informalmente como *flash notation*. La notación representa la longitud de la máscara en valor decimal y utiliza una diagonal para separar este valor de la dirección. Por lo tanto, en notación CIDR el bloque de direcciones de la Tabla 3 se representa como:

128.211.168.0/21

Donde /21 denota 21 bits de máscara. La tabla 37 enlista el formato decimal para todas las máscaras CIDR posibles. Los prefijos /8, /16 y /24 corresponden a las tradicionales clases A, B y C.

Notación CIDR	Notación Decimal	Notación CIDR	Notación Decimal
/1	128.0.0.0	/17	255.255.128.0
/2	192.0.0.0	/18	255.255.192.0
/3	224.0.0.0	/19	255.255.224.0
/4	240.0.0.0	/20	255.255.240.0
/5	248.0.0.0	/21	255.255.248.0
/6	252.0.0.0.	/22	255.255.252.0
/7	254.0.0.0	/23	255.255.254.0
/8	255.0.0.0	/24	255.255.255.0
/9	255.128.0.0	/25	255.255.255.128
/10	255.192.0.0	/26	255.255.255.192
/11	255.224.0.0	/27	255.255.255.224
/12	255.240.0.0	/28	255.255.255.240
/13	255.248.0.0	/29	255.255.255.248
/14	255.252.0.0	/30	255.255.255.252
/15	255.254.0.0	/31	255.255.255.254
/16	255.255.0.0	/32	255.255.255.255

Tabla 37. Valores de la máscara en notación decimal y todos los prefijos CIDR posibles

1.5.3.3.4 Bloques CIDR Reservados para Redes Privadas

Los prefijos reservados nunca serán asignados a las redes en la red pública de Internet, estos son conocidos como direcciones privadas o direcciones no enrutables. Este ultimo

concepto debido a que los enrutadores en la red de Internet entienden que estas direcciones están reservadas, si un paquete destinado a alguna dirección privada es accidentalmente enrutado hacia la red de Internet, cualquier enrutador en Internet podrá detectar el problema. Además, que los bloques que corresponden a las direcciones classful, el bloque de prefijos reservados para IPv4 contienen un bloque CIDR que abarca diversas clases. La tabla 6 enlista los valores en notación CIDR con su respectivo valor en notación decimal de la dirección menor y mayor. La última dirección enlistada en el bloque, 169.254/16, no es usada debido a que esta es utilizada por los sistemas que autoconfiguran direcciones IP. Esto se define en el RFC 1918.

Prefijo	Dirección menor	Dirección mayor
10/0	10.0.0.0	10.255.255.255
172.16/12	172.16.0.0	172.16.255.255
192.168/16	192.168.0.0	192.168.255.255
169.254/16	169.254.0.0	169.254.255.255

Tabla 38. Prefijos utilizados para las redes privadas que o son utilizadas en la red Internet. Si un paquete enviado a alguna de estas direcciones arriba accidentalmente a Internet, ocurrirá un problema.

CIDR representa el mayor progreso en tecnología IP. En lugar de considerar las clases originales de red, el direccionamiento classless permite la división entre el prefijo y el sufijo ocurra en un bit frontera. Además, permite que el espacio de direcciones sea dividido en bloques, donde el tamaño del bloque esta conformado de dos elementos. Una de las principales motivaciones para que CIDR creciera fue el deseo de combinar varios prefijos de clase C en un solo bloque de superred. Debido a que las direcciones classles no se identifican por si mismas como las direcciones classful. CIDR requiere de cambios significativos en los algoritmos y en la estructuras de datos que utiliza el software IP en los hosts y en los enrutadores para guardar y conocer enrutadores.

1.5.3.4 NAT (*Netwok Address Translation*

Internet a crecido más de lo imaginable, su tamaño exacto no se conoce, una estimación actual indica que hay alrededor de 100 millones de hosts y más 350 millones de usuarios activos en Internet. Esta cantidad es mayor que la población de Estados Unidos. Es un hecho que la razón de crecimiento de Internet es el doble de tamaño cada año.

Con la explosión de Internet y el incremento de las LANs y las redes de negocios, el número de direcciones IP no es suficiente. La solución obvia es rediseñar el formato de direcciones para permitir más direcciones posibles. Esto se esta desarrollando (IPv6), pero su implementación tomará muchos años debido a que se requiere de modificaciones en la infraestructura de Internet.

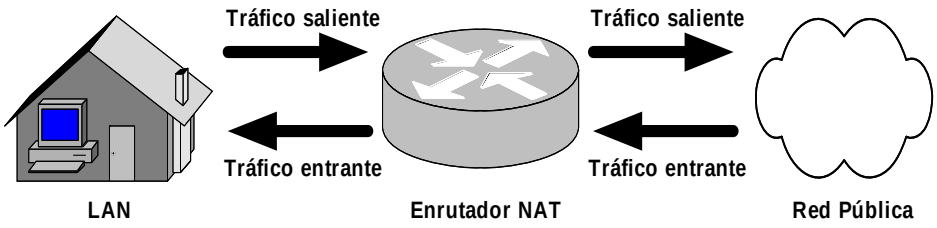


Figura 66. El enrutador NAT traduce el tráfico entrante y saliente de la red privada

NAT (*Network Address Translation*) es una solución para este tipo de problemas. La traducción de direcciones de red permite que un dispositivo único, como lo es un enrutador, actúe como agente entre Internet (o la red pública) y una red LAN (o privada). Esto significa que una dirección IP pública (dirección homologada) se requiere para representar a un grupo entero de hosts.

1.5.3.4.1 ¿Cómo trabaja NAT?

NAT fue desarrollado por Cisco y es usado por un dispositivo (puede ser un enrutador, firewall o host) y permite la comunicación entre las LANs y el resto del mundo. NAT tiene diversas formas y puede trabajar de diferentes maneras:

- NAT Estático: Traduce una dirección IP privada hacia una dirección IP homologada en una arquitectura uno a uno.

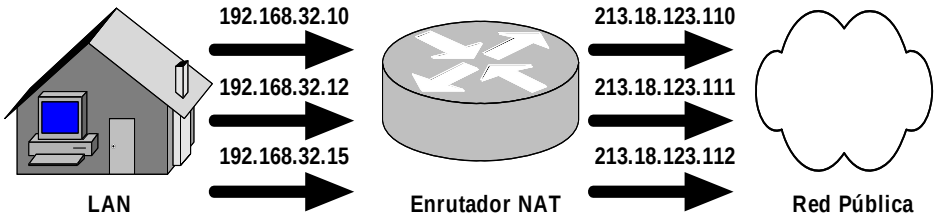


Figura 67. Con NAT Estático, el host con la dirección IP 192.168.32.10 siempre será traducida con la dirección IP 213.18.123.110

- NAT Dinámico: Traduce una dirección IP privada hacia una dirección IP homologada que pertenece a un grupo de direcciones IP homologadas.

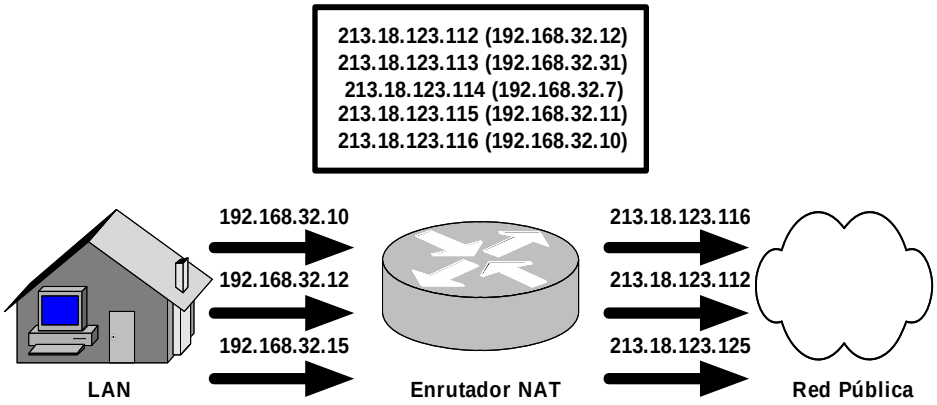


Figura 68. Con NAT dinámico, el host con la dirección IP 192.168.32.10 será traducida con la primera dirección disponible en el rango de 21.18.123.100 a 213.18.123.150

- PAT (*Port Address Translation*): es una forma del NAT Dinámico que traduce direcciones IP multiples privadas hacia una única dirección IP homologada usando diferentes puertos. Esta variante también es conocida como *Overloading*, NAT con dirección única o NAT con multicanalización de puertos.

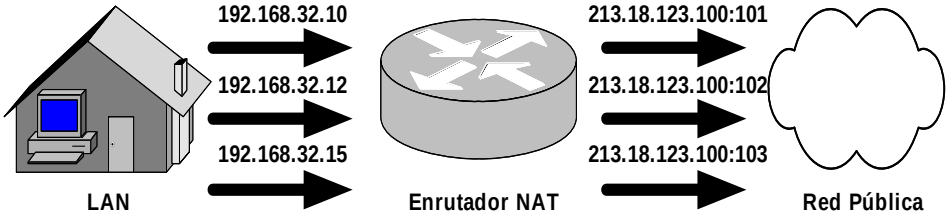


Figura 69. Con PAT, cada dirección IP de los hosts de la LAN es traducida a la misma dirección IP (213.18.123.100), pero asignándole un número de puerto diferente

- *Overlapping:* Cuando las direcciones IP de una LAN son direcciones homologadas que son usadas en otra LAN, el enrutador debe mantener una tabla de traducción de direcciones con esas direcciones para poder interceptarlas y traducirlas por direcciones IP homologadas y únicas. Es importante notar que el enrutador NAT debe traducir las direcciones IP internas en direcciones homologadas y únicas, al igual que traducir las direcciones externas homologadas en direcciones que son únicas para la LAN. Esto puede también lograrse usando NAT estático o usando DNS e implementando NAT dinámico.

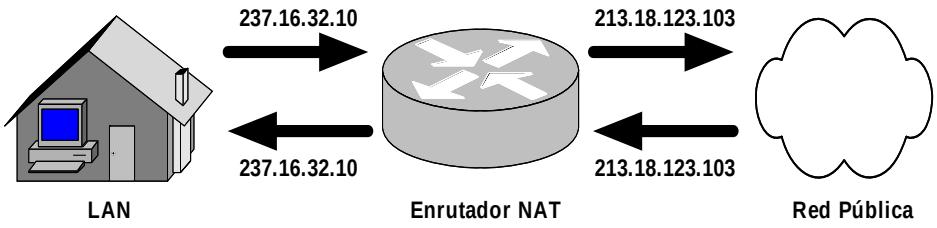


Figura 70. El rango interno IP (237.16.32.XX) es un rango de direcciones homologadas usado por otra red. Por lo tanto, el enrutador traduce las direcciones para evitar un conflicto potencial con otra red. El enrutador también traduce las direcciones homologadas en direcciones privadas cuando la información es enviada hacia la LAN

Una LAN que usa direccionamiento IP interno se le conoce con el concepto de *stub domain*. La mayor parte del tráfico de red en una LAN es tráfico local, por lo tanto este no viaja fuera de la LAN. Una red LAN puede contener direcciones IP homologadas y privadas. Un host que usa una dirección IP privada tiene que usar NAT para comunicarse con el resto del mundo.

NAT puede ser configurado de varias maneras. En la siguiente figura, el enrutador NAT esta configurado para traducir direcciones IP privadas (locales) que residen en la LAN hacia direcciones IP homologadas. Esto ocurre siempre y cuando cualquier dispositivo en la LAN con dirección IP privada necesita comunicarse con la red pública.

- Un proveedor de servicios de Internet asigna un rango de direcciones a las compañías. El conjunto asignado de estas direcciones privadas, son direcciones IP únicas y son llamadas direcciones globales de la LAN (*inside global addresses*). Las direcciones privadas son divididas en dos grupos. El primer grupo debe ser usado por los enrutadores NAT (*outside local addresses*), el siguiente grupo, mucho más grande y conocido como direcciones locales de la LAN (*inside local addresse*s) debe ser usado en el *stub domain.* Las direcciones de los enrutadores NAT son usadas para traducir las direcciones IP únicas de los dispositivos de la red pública (*outside global addresses*).

La mayoría de los hosts de la LAN se comunica con cualquier otro host usando las direcciones locales de la LAN. Algunos hots de la LAN se comunican con otros hosts que se encuentran fuera de la LAN. Estos hosts tienen direcciones homologadas dentro de la LAN, lo cual significa que estas direcciones no requieren de traducción de direcciones de red. Cuando un host de la LAN que tiene una dirección privada quiere comunicarse más allá de la LAN, el paquete fluye hacia uno de los enrutadores NAT. El enrutador NAT checa su tabla de traducción de direcciones para ver si conoce la dirección IP destino. Si la conoce, el enrutador NAT traduce el paquete y crea una entrada en la tabla de traducción de direcciones para él. Si la dirección IP destino no esta en la tabla de traducción de direcciones, el paquete es desechado. Usando una dirección homologada de LAN, el enrutador envía el paquete hacia su destino. El enrutador NAT checa en su tabla de traducción de direcciones y determina que la dirección destino esta ahí y enruta hacia una dirección de un host en la LAN. Este enrutador traduce las direcciones homologadas del paquete hacia las direcciones privadas de LAN y lo envía hacia el host destino.

PAT utiliza una característica de TCP/IP, la multicanalización, que permite a un host mantener varias conexiones con uno o varios hosts remotos usando los diferentes puertos TCP o UDP. Como el paquete IP contiene las direcciones IP origen y destino, así como el número de puertos origen y destino. Las direcciones IP caracterizan a cada host, mientras que los números de puerto, aseguran que la conexión entre ambos hosts tenga un identificador único. La combinación de estos cuatro números definen la conexión TCP/IP.

1.5.3.4.2 ¿Cómo trabaja PAT (*Port Address Translation*)?

Si tenemos una LAN que usa direcciones IP privadas que no fueron asignadas por la IANA (*Internet Assigned Numbers Authority*), estas direcciones no son únicas. La compañía instala un enrutador NAT, este tendrá una dirección homologada y única asignada por la IANA. Cuando un host de la LAN intenta conectarse con un host fuera de la LAN, por ejemplo un servidor Web. El enrutador recibe el paquete del host, salva la dirección IP privada del host y el número de puerto en una tabla de traducción de direcciones. El enrutador reemplaza la dirección IP privada del host con su propia dirección, también reemplaza el número del puerto origen con el número del puerto correspondiente a la entrada de información salvada en la tabla de traducción de direcciones. La tabla de traducción tiene ahora bien ubicado al host: con su dirección IP privada y el número de puerto con la dirección IP del enrutador. Cuando el paquete regresa desde el host destino, el enrutador verifica el puerto destino en el paquete, después verifica en su tabla de traducción de direcciones, a que host de la LAN pertenece el paquete. El enrutador cambia la dirección destino y el puerto destino con los que salvo en su tabla y envía el paquete hacia el host de la LAN. El host recibe el paquete y el procedimiento se repite mientras el host mantiene la comunicación con el dispositivo externo. Una vez que el enrutador NAT conoce la dirección fuente del host y el puerto fuente salvados en la tabla de traducción de direcciones, este puede seguir usando el mismo número de puerto mientras dure la conexión Un contador de tiempo es reiniciado cada vez que el enrutador accesa una entrada en esta tabla. Si la entrada no se necesita nuevamente antes de que el contador de tiempo expire, la entrada es removida de la tabla.

En la siguiente tabla podemos ver como los hosts de la LAN pueden aparecer para las redes externas o Internet.

Host Fuente	Dirección IP del host fuente	Puerto fuente del host	Dirección IP del enrutador NAT	Número de Puerto asignado por el enrutador NAT
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

Tabla 39. Tabla de traducción de direcciones de un enrutador

Como se puede ver, el enrutador NAT almacena la dirección IP y el número de puerto de cada host en la tabla de traducción de direcciones. El enrutador reemplaza la dirección IP con su propia dirección IP pública y el número de puerto con la correspondiente localización de la entrada de los paquetes del host origen, en dicha tabla. Las redes externas ahora verán la dirección IP y el puerto del enrutador NAT como el origen de cada paquete de información.

Se pueden tener algunos hosts que utilicen direcciones IP dedicadas dentro de la LAN. Se puede crear una lista de acceso, la cual le diga al enrutador que hosts de la LAN requieren NAT, las direcciones IP restantes pasarán sin ser traducidas por el enrutador NAT.

El número de traducciones simultáneas que un enrutador soporta, es determinado principalmente por la cantidad de DRAM (*Dynamic Random Access Memory*). Pero debido a que una entrada típica en la tabla de traducción de direcciones solo requiere alrededor de 160 bytes, un enrutador con 4Mb de DRAM teóricamente procesaría 26214 traducciones simultáneamente, lo cual es más que suficiente para varias aplicaciones.

La IANA tiene rangos específicos de direcciones IP no enrutables, direcciones internas de red o direcciones privadas. Este tipo de direcciones se consideran direcciones no homologadas (RFC 1918: *Address Allocation for Private Networks*). Ninguna compañía o agencia puede adueñarse de estas direcciones y usarlas en hosts públicos. Los enrutadores son diseñados para descartar a las direcciones privadas, lo que significa que si un paquete de un host con dirección IP privada quiere establecer comunicación con un host con dirección homologada, este paquete será descartado por el primer enrutador al que arrive dicho paquete.

1.5.3.5 Multicast

Cuando una aplicación necesita enviar datos a más de una estación, pero quiere restringir el envío solo para las estaciones interesadas en recibir este tráfico, la aplicación típica utiliza una dirección de destino multicast. Las direcciones multicast realizan un subarreglo de todas las estaciones en una red. Los otros dos tipos de transmisión para los equipos de transmisión son los paquetes de unicast o broadcast. Si la fuente usa una dirección de broadcast, todas las estaciones en el dominio de broadcast deben procesar el paquete, aún si ellos no están interesados en la información. Si la fuente transmite paquetes de unicast, debe de enviar muchas copias del paquete, cada uno direccionado hacia el destino planeado. Este es un uso ineficiente de los recursos de la red y eso no es escalable cuando el número de usuarios se incrementa.

Usando direcciones multicast, la fuente trasmite solo una copia del paquete sobre los enrutadores distribuyen el mensaje multicast hacia los demás segmentos donde se encuentran los receptores interesados en ese paquete. Las direcciones multicast actúan en capa 2 y capa 3 del modelo OSI. El administrador de red asigna las direcciones multicast de capa 3 para aplicaciones. Las direcciones multicast de capa 2 son calculadas a partir de las direcciones multicast de capa 3. Cuando configuramos una aplicación multicast, la tarjeta de red (NIC) agrega la dirección multicast a su lista de direcciones MAC validas. Comúnmente esta lista consiste en la suma de la dirección MAC local y de algunas direcciones configuradas de los usuarios. Cuando una estación recibe un paquete con una dirección destino multicast, esta envía el paquete hacia el CPU.

Los enrutadores examinan las direcciones multicast de capa 2 y capa 3, mientras que un switch solo examina las direcciones multicast de capa 2. Si, un switch posee hardware como un modulo de supervisor adicional, puede examinar también las direcciones multicast de capa 3. De lo contrario, simplemente examina las direcciones MAC en la trama.

1.5.3.5.1 Direcciones Multicast de Capa 3

La direcciones IP multicast de capa 3 son caracterizadas como direcciones de clase D. Los primeros cuatro bits de las direcciones clase D son 1110. Esto significa que las direcciones IP multicast tienen una rango válido de la dirección 224.0.0.0 a la dirección 239.255.255.255. Debemos saber que las direcciones IP multicast que se encuentran en el rango de 224.0.0.0 a 224.0.0.255 están reservadas. Las siguientes tres direcciones son importantes:

- **224.0.0.1** – Todos los host posibles de multicast en el segmento
- **224.0.0.2** – Todos los enrutadores de multicast posibles en el segmento
- **224.0.0.4** – Todos los enrutadores DVMRP (*Distance Vector Multicast Routing Protocol*) en el segmento

Comúnmente, el administrador de red asigna direcciones multicast a las aplicaciones y debe seleccionar aquellas direcciones que no están en uso por otras aplicaciones o procesos. El administrador no debe usar direcciones multicast del rango de direcciones reservadas.

1.5.3.5.2 Direcciones Multicast de Capa 2

Cuando se asigna direcciones multicast de capa 3, las direcciones de capa dos son automáticamente generadas a partir de la dirección IP. La figura 71 muestra como una dirección MAC de multicast se deriva de una dirección IP multicast. Para calcular la dirección de capa 2, el host copia los últimos 23 bits de la dirección IP multicast y los coloca en los últimos 24 bits de la dirección MAC, dejando en cero al bit de mayor orden.

Los tres primeros bytes (24 bits) de la dirección MAC multicast son 0x01-00-5E. Este es un valor OUI reservado que indica una aplicación multicast.

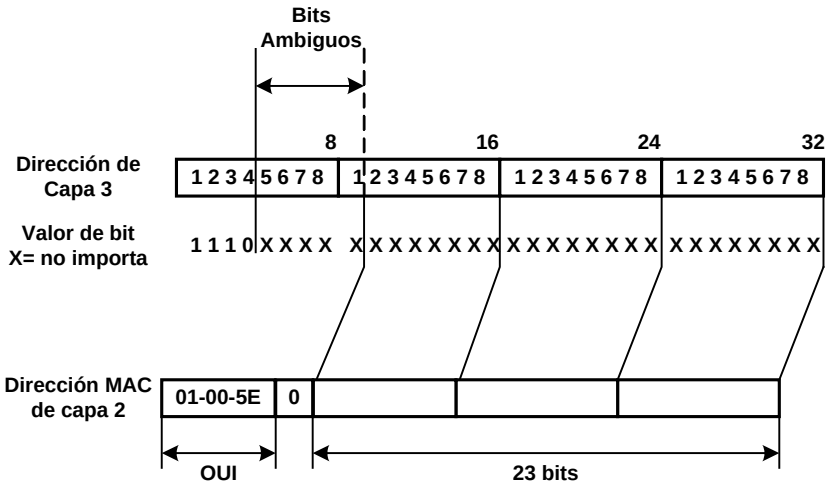


Figura 71. Calculando una dirección MAC multicast

Si se tiene la dirección IP 224.1.10.10, asignada por el administrador, el valor de los 23 bits menores es de 1.10.10. En formato hexadecimal es de 0x01-0A-0A. La dirección MAC toma los últimos 23 bits colocándolos en el campo MAC. La dirección MAC completa para este caso es 01-00-5E-01-0A-0A.

¿Qué pasa si la dirección IP multicast es 225.1.10.10? Un efecto de este esquema es la ambigüedad en direcciones. A pesar de que un grupo IP multicast diferente es identificado en capa 3, la dirección de capa 2 es la misma que 224.1.10.10. Los equipos de capa 2 no pueden distinguir los dos grupos multicast, y por lo tanto, reciben tramas de ambos grupos. La aplicación usada por el usuario necesita un filtro para poder descartar las tramas del grupo multicast no deseado. Alguna combinación de bits para los 5 bits identificados en la figura 1 como ambiguos, generan la misma dirección MAC multicast de capa 2. Cinco bits significa que existen 2^5 combinaciones posibles, o 32 direcciones de capa 3 que crean la misma dirección de capa 2.

Cuando se asignan direcciones multicast debemos recordar la ambigüedad 32:1 y tratar de evitar el traslape multicast. Esto nos ayudara a conservar el ancho de banda para poder acceder a los enlaces troncales. La estación final descartara el multicast no requerido de capa 3, después interrumpirá al CPU.

1.6 Protocolos de Enrutamiento IP

1.6.1 ARP

El Protocolo de Resolución de Direcciones (*ARP: Address Resolution Protocol*, RFC 826) es un protocolo utilizado en la resolución de direcciones de enlace (direcciones físicas) a partir de direcciones de red. ARP está diseñado para soportar diferentes protocolos de enlace y de red. Por lo tanto, el protocolo ARP es un sencillo protocolo que a partir de una dirección de red (dirección IP) obtiene su correspondiente dirección física (dirección Ethernet o también llamadas: *MAC address*). Esto ocurre siempre así cuando un host usando TCP/IP quiere enviar información a otro host de su red local. El host que quiere

enviar la información no le basta con conocer la dirección IP del host destino, ya que la tarjeta de red no entiende de direcciones IP, sino que tan sólo reconoce direcciones definidas por la interfaz de acceso al medio que implementa, por ejemplo Ethernet.

Dentro de una misma red, las máquinas se comunican enviándose tramas físicas. Las tramas Ethernet contienen campos para las direcciones físicas de origen y destino (6 bytes cada una):

8 bytes	6 bytes	6 bytes	2 bytes	64-1500 bytes	4 bytes
Preámbulo	Dirección física destino	Dirección física origen	Tipo de trama	Datos de la trama	CRC

Tabla 40. Trama Ethernet

El problema que se nos plantea es cómo se puede conocer la dirección física de la máquina destino. El único dato que se indica en los datagramas es la dirección IP de destino. ¿Cómo se pueden entregar entonces estos datagramas? Se necesita obtener la dirección física de un ordenador a partir de su dirección IP. Esta es justamente la misión del protocolo.

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
E1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
E2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

Tabla 41. Interconexión de 3 redes mediante enrutadores, sus direcciones físicas y direcciones IP.

Considerando la tabla anterior. El host A envía un datagrama con origen 192.168.0.10 y destino 10.10.0.7 (B). Como el host B se encuentra en una red distinta al host A, el datagrama tiene que atravesar el enrutador 192.168.0.1 (E1). Se necesita conocer la dirección física de E1. Es entonces cuando entra en funcionamiento el protocolo ARP: A envía un mensaje ARP a todas las máquinas de su red preguntando "¿Cuál es la dirección física de la máquina con dirección IP 192.168.0.1?". La máquina con dirección 192.168.0.1 (E1) advierte que la pregunta está dirigida a ella y responde a A con su dirección física (00-E0-4C-AB-9A-FF). Entonces A envía una trama física con origen 00-60-52-0B-B7-7D y destino 00-E0-4C-AB-9A-FF conteniendo el datagrama (origen 192.168.0.10 y destino 10.10.0.7). Al otro lado del enrutador E2 se repite de nuevo el

proceso para conocer la dirección física de B y entregar finalmente el datagrama a B. El mismo datagrama ha viajado en dos tramas físicas distintas, una para la red 1 y otra para la red 2.

Se puede observar que las preguntas ARP son de difusión (se envían a todas las máquinas). Estas preguntas llevan además la dirección IP y dirección física de la máquina que pregunta. La respuesta se envía directamente a la máquina que formuló la pregunta.

1.6.1.1 Tabla ARP (Caché ARP)

Cada host almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada en su tabla. La primera vez que C envíe un mensaje a D tendrá que difundir previamente una pregunta ARP, tal como hemos visto. Sin embargo, las siguientes veces que C envíe mensajes a D ya no será necesario realizar nuevas preguntas puesto que C habrá almacenado en su tabla la dirección física de D. Sin embargo, para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla.

Las tablas ARP reducen el tráfico de la red al evitar preguntas ARP innecesarias. Pensemos ahora en distintas maneras para mejorar el rendimiento de la red. Después de una pregunta ARP, el destino conoce las direcciones IP y física del origen. Por lo tanto, podría insertar la correspondiente entrada en su tabla. Pero no sólo eso, sino que todas las estaciones de la red escuchan la pregunta ARP: podrían insertar también las correspondientes entradas en sus tablas. Como es muy probable que otras máquinas se comuniquen en un futuro con la primera, habremos reducido así el tráfico de la red aumentando su rendimiento.

Esto que se ha explicado es para comunicar dos máquinas conectadas a la misma red. Si la otra máquina no estuviese conectada a la misma red, sería necesario atravesar uno o más enrutadores hasta llegar al host destino. La máquina origen, si no la tiene en su tabla, formularía una pregunta ARP solicitando la dirección física del enrutador y le transferiría a éste el mensaje. Estos pasos se van repitiendo para cada red hasta llegar a la máquina destino.

1.6.2 Proxy ARP o Subnetting Transparente

El Proxy-ARP se describe en el RFC 1027 - *Usando ARP para implementar pasarelas de subredes transparentes*-, que de hecho es un subconjunto del método propuesto en el RFC 925 - *Resolución de Direcciones Multi-LAN*-. Es otro método para construir subredes locales, sin necesidad de modificar el algoritmo de encaminamiento IP, pero con modificaciones en los enrutadores, que interconectan las subredes.

1.6.2.1 Concepto de Proxy ARP

Los términos *ARP sustituto (Proxy ARP), promiscuo o ARP hack,* se refieren a la segunda técnica utilizada para transformar un solo prefijo IP de red en dos direcciones físicas. La técnica, que sólo se aplica en redes que utilizan ARP para convertir direcciones de red en direcciones físicas, se puede explicar mejor mediante un ejemplo. En la figura 72 se ilustra la situación.

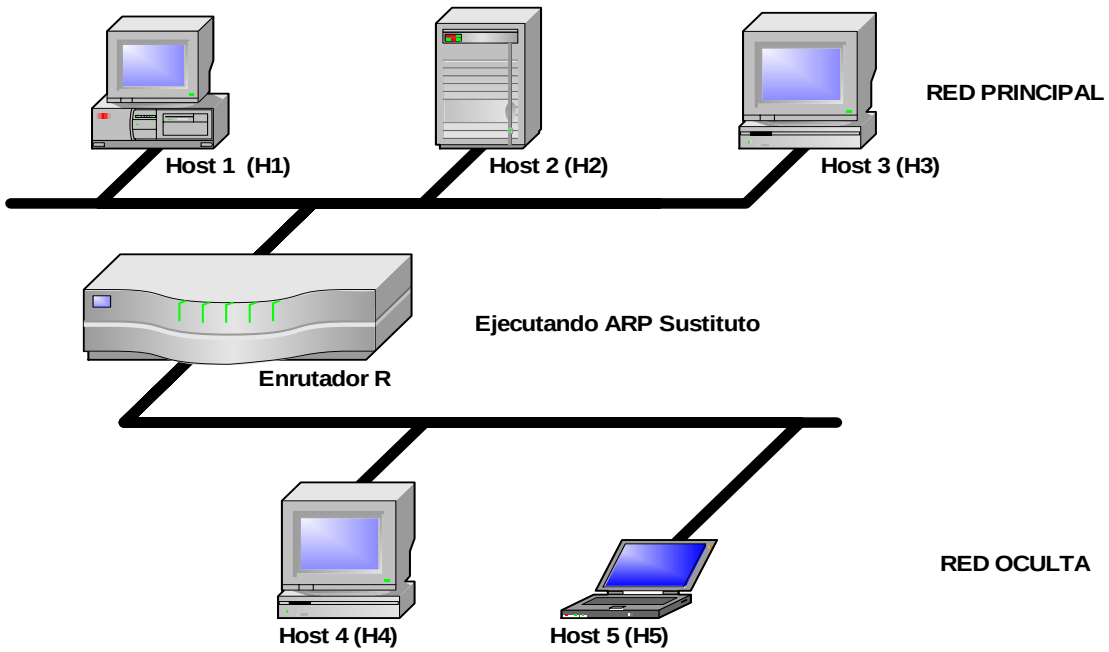


Figura 72. La técnica de ARP sustituto (ARP hack) permite que una dirección de red se comparta entre dos redes físicas. El enrutador R contesta solicitudes ARP en cada red para los anfitriones en otra, proporcionando su dirección de hardware y enrutando datagramas de manera correcta en cuanto llegan. En esencia, R miente sobre las transformaciones de dirección IP a dirección física.

Dos redes comparten una sola dirección IP. Imaginese que la etiquetada como *Red Principal* era la red original y segunda, etiquetada como *Red Oculta,* se agregó después. R, que es el enrutador que conecta las dos redes, sabe qué hosts residen en cada red física y utiliza ARP para mantener la ilusión de que solamente existe una red. Para dar esa apariencia, R mantiene totalmente oculta la localización de los hosts, permitiendo que las demás máquinas en la red se comuniquen como si estuvieran conectadas de manera directa. En el ejemplo, cuando el host H1 necesita comunicarse con el host H4**,** primero llama a ARP para convertir la dirección IP de H4 en una dirección física. Una vez que tiene la dirección física, H1 puede enviarle directamente el datagrama.

Debido a que el enrutador R corre software Proxy ARP, R captura la solicitud transmitida por difusión de H1 decide que la máquina en cuestión reside en la otra red física y responde la solicitud ARP enviando su propia dirección física. H1 recibe la respuesta ARP, instala la asociación en su tabla ARP y la utiliza para enviar a R los datagramas destinados a H4**.** Cuando R recibe un datagrama, busca en una tabla especial de

enrutamiento para determinar cómo enrutar el datagrama. R debe encaminar los datagramas destinados a *H4* a través de la red oculta. a fin de permitir que los hosts en la red oculta alcancen hosts en la red principal, R también realiza el servicio de ARP sustituto (Proxy ARP) en dicha red.

Los enrutadores que utilizan la técnica de ARP sustituto, tornan ventaja de una característica importante del protocolo ARP, a saber, la confianza. ARP está basado en la idea de que todas las máquinas cooperan y de que cualquier respuesta es legítima. La mayor parte de los hosts instalan asociaciones obtenidas por medio de ARP sin verificar su validez y sin mantener una consistencia. Por lo tanto, puede suceder que la tabla ARP asocie muchas direcciones IP en la misma dirección física, sin embargo, esto no viola las especificaciones del protocolo.

Algunas implantaciones de ARP no son tan poco exigentes como otras. En particular, las implementaciones ARP diseñadas para alertar a los administradores de posibles violaciones de seguridad les informarán siempre que dos direcciones IP distintas se transformen en la misma dirección física de hardware. El propósito de alertar al administrador es avisarle sobre el *spoofing,* situación en la que una máquina indica ser otra para poder interceptar paquetes. Las implantaciones de ARP en hosts que alertan a los administradores del posible *spoofing* no se pueden utilizar en redes que tienen enrutadores sustitutos ARP, ya que el software generarla mensajes con gran frecuencia.

La principal ventaja de ARP sustituto es que se puede agregar a un solo enrutador en una red sin alterar las tablas de enrutamiento en otros hosts o enrutadores en esa red. Por lo tanto, el software ARP sustituto (Proxy ARP) oculta completamente los detalles de las conexiones físicas.

La principal desventaja de ARP sustituto es que no trabaja para las redes a menos que utilicen ARP para la definición de direcciones. Además, no se generaliza para topologías de red más complejas (por ejemplo, muchos enrutadores que interconectan dos redes físicas), ni incorpora una forma razonable para el enrutamiento. De hecho, la mayor parte de las implantaciones de ARP confía en los administradores para el mantenimiento manual de máquinas y direcciones, haciendo que se ocupe tiempo y se tenga propensión a los errores.

1.6.3 Gratuitous ARP

Cada vez que un host inicia la configuración de una interface de red que hace uso del protocolo ARP, el protocolo ARP envía un paquete ARP con el fin de determinar si su dirección IP o dirección física está siendo utilizada por otro host (detectando direcciones IP duplicadas) y así ofrecer la oportunidad a los demás hosts de actualizar su caché ARP.

En un paquete ARP gratuito la dirección física destino es igual a la dirección física Fuente, y la dirección IP destino es igual a la dirección IP fuente. Si algún host de la red local detecta un paquete ARP gratuito cuya dirección IP es la misma que la configurada en su interface de red el mismo envía un paquete ARP indicando su dirección IP y dirección física al host que transmitió el ARP gratuito. De esta manera el host que envió el ARP gratuito genera un mensaje de advertencia indicando que dicha dirección IP está siendo utilizada por otro host.

1.6.4 Enrutamiento por Vector de Distancia (*Distance Vector*)

Este tipo de protocolos de enrutamiento mantiene una tabla con las mejores distancias y líneas a cada destino, actualiza sus tablas de enrutamiento intercambiando información con lo enrutadores vecinos. La tabla almacena una entrada para cada enrutador en la subred, las tablas almacenan la línea preferida de salida y una estimación del tiempo o la distancia destino. Cada enrutador sabe las distancias a sus vecinos, por ejemplo si la métrica es el retraso el enrutador la puede medir con paquetes de eco. Cada T en ms los enrutadores intercambian sus tablas con sus vecinos. Cada enrutador usa las tablas de sus vecinos y las mediciones de las distancias a sus vecinos para calcular una nueva tabla.

Cada enrutador calcula el mejor camino a todos los destino y lo informa a los demás, informa la dirección y distancia (métrica) a un destino. La dirección es generalmente a través del enrutador que hace el anuncio, el cálculo es simple, incremental y distribuido, como ejemplos tenemos: RIP, IPX-RIP, DECnet, IGRP, EIGRP (incluye capacidades típicas de protocolos Link-State).

1.6.4.1 Routing Information Protocol (RIP)

Uno de los protocolos de enrutamiento más antiguos es RIP. Este protocolo utiliza algoritmos de vector distancia para calcular sus rutas. Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson. La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP *(Gateway Information Protocol)*, este protocolo estaba incluido dentro de la arquitectura *XNS (Xerox Network Systems)*. GIP se utilizaba para intercambiar información de enrutamiento entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario. Poco después la Universidad de California en Berkeley creo una variante llamada "routed", esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible, también se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

El protocolo RIP, fue descrito por primera vez en el RFC 1058 por C. Hedrick de la Rutgers University en Junio de 1988, y posteriormente fue mejorado en la RFC 2453 por G.Malkin de la compañía Bay Networks en Noviembre de 1998. Desde el año 1998 el protocolo RIP se ha mantenido estable, aunque posteriormente salió la versión para Ipv6, la cual tiene su propio capítulo.

RIP es un protocolo de enrutamiento de vector de distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de

enrutamiento como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies. RIP busca su camino óptimo mediante el conteo de saltos, considerando que cada enrutador atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

El protocolo RIPv1, al igual que sus antecesores propietarios fue diseñado para funcionar como protocolo vector distancia en redes pequeñas de pasarela interior. RIPv1 está basado según el autor del RFC en la versión 4.3 de la distribución de UNIX de Berkeley.

En cuanto al protocolo se tienen que tener en cuenta las tres limitaciones:

- El protocolo no permite más de quince saltos, es decir, los dos enrutadores más alejados de la red no pueden distar más de 15 saltos, si esto ocurriera no sería posible utilizar RIP en esta red.
- Problema del "conteo a infinito". Este problema puede surgir en situaciones atípicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado. El autor del RFC 1058 también comenta que en la realidad esto sólo puede ser un problema en redes lentas, pero el problema existe.
- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de parámetros en tiempo real como por ejemplo retardos o carga del enlace.

Además de los problemas que cita el autor del protocolo, se debe tomar en cuenta que el protocolo RIPv1 es un protocolo classfull, con lo que existe el problema de la discontinuidad de redes. El problema de la discontinuidad de redes se produce en el momento que se tiene una red dividida en varias subredes y no pueden ser sumarizadas en una misma ruta, ya que físicamente cada una de las subredes está ubicada en un lugar que depende de un interfaz distinto una subred de la otra. Pero claro, en la época en la que se escribió este RFC, que era en 1988 estos problemas no estaban contemplados y con el tiempo se detectó este problema, esta es una de las razones de la existencia de RIPv2.

La base de datos de enrutamiento de cada uno de los hosts de la red que están utilizando el protocolo de enrutamiento RIP tiene los siguientes campos:

Dirección de destino
La dirección de destino en la tabla de enrutamiento de RIP será la red destino, es decir, la red final a la que deseamos acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente clasfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subnetting en RIP versión 1, por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classfull la red de destino tiene 256 direcciones, de las cuales 254 son útiles, una vez descontada la dirección de red y la dirección broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts de dentro de la red.

Siguiente salto
El siguiente salto lo definimos como el siguiente enrutadorr por el que nuestro paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un enrutador vecino del enrutador origen.

Interfaz de salida del enrutador
Entendemos por interfaz de salida del enrutador al interfaz al cual está conectado su siguiente salto.

Métrica
La métrica utilizada por RIP consiste en el conteo de saltos, como métrica se considera cada salto como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la línea. La métrica total consiste en el total de saltos desde el enrutador origen hasta el enrutador destino, con la limitación que 16 saltos se considera destino inaccesible, esto limita el tamaño máximo de la red.

Temporizador
El temporizador indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización que se estable 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 se considera al tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos. El tiempo de desactivación se considera al tiempo máximo que puede esperar un enrutador sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y con lo cual el enrutador no está activo en la red, se establece la métrica a valor 16, es decir destino inalcanzable. El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese enrutador supuestamente caído son eliminadas de la tabla de enrutamiento.

Para obtener esta tabla, RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de enrutamiento de cada uno de los nodos o enrutadores de la red:

- Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del enrutador a esa red. Conceptualmente también debería de existir una entrada para el enrutador mismo con métrica 0, pero esta entrada no existirá.
- Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del enrutador mediante la dirección broadcast. Esta actualización contendrá toda la tabla de enrutamiento.
- Cuando llegue una actualización desde un vecino S, se añadirá el coste asociado a la red de S, y el resultado será la distancia D'. Se comparará la distancia D y si es menor que el valor actual de D a esa red entonces se sustituirá D por D'.

Diez años después de que se publicara la versión 1 de RIP se publicó la versión 2, por G. Malkin de la compañía Bay Networks en Noviembre de 1998 en el RFC 2453. RIPv2 establece una serie de mejoras muy importantes con su antecesor que son las siguientes:

- Autenticación para la transmisión de información de RIP entre vecinos.
- Utilización de mascaras de red, con lo que ya es posible utilizar VLSM.
- Utilización de máscaras 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 Multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de información de gestión (MIB).

Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de enrutamiento.

Pero RIPv2 aunque haya tenido una serie de mejoras muy importantes desde la versión 1 del protocolo sigue teniendo una serie de carencias muy importantes como:

- Limitación en el tamaño máximo de la red. Con RIPv2 sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, lo cual implica que no nos permite la utilización de RIPv2 en redes de un tamaño más grande.
- Conteo a infinito, RIPv2 sigue sin solucionar el problema del conteo hasta el infinito si se forman bucles, aunque existen técnicas externas al protocolo como pueden ser la inversa envenenada y el horizonte dividido, técnicas brevemente descritas por William Stallings en su libro "Comunicaciones y Redes de Computadoras", las cuales consisten básicamente en no anunciar una ruta por el interfaz por el que se ha recibido en algún momento.
- Métricas estáticas que pueden ser cambiadas por el administrador de la red, pero que no nos dan ninguna información del estado de la red.
- RIPv2 sólo permite al igual que su antecesor una ruta por cada destino, lo cual implica la imposibilidad de realizar balanceos de carga por ejemplo, lo que redunda en una pobre y poco óptima utilización de los enlaces.
- RIPv2 es un protocolo que al igual que su antecesor genera muchísimo tráfico al enviar toda la tabla de enrutamiento en cada actualización, con la carga de tráfico que ello conlleva.

1.6.5 Enrutamiento por Estado de Enlace (*Link-State*)

Aproximación de base de datos distribuida replicada en vez de un cálculo distribuido Incremental. Los enrutadores informan de sus enlaces a redes activos y con enrutadores vecinos, la red se inunda con esta información para que llegue a todos los enrutadores obteniendo información sobre toda la topología, tienen una imagen de la red (todos la misma) y a partir de ahí eligen los caminos. Este tipo de Protocolos tienen menor tiempo de convergencia que los protocolos de enrutamiento por vector de distancia ante cambios en la red, sobre el grafo se suele emplear el algoritmo de Dijkstra para calcular las rutas, ejemplos: OSPF, IS-IS, PNNI.

1.6.5.1 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF), es un protocolo de enrutamiento por estado de enlace basado en una norma abierta. OSPF ha sido descrito en varios RFCs, pero la norma de OSPF v.2 está descrito por John J. Moy en el RFC2328 y en el libro "*OSPF Anatomy of an*

Internet Routing Protocol", escrito por el mismo autor, y publicado por la editorial Addison-Wesley.

El término Open en el nombre del protocolo hace referencia a que es un protocolo abierto al público y no propietario de ninguna compañía. De entre los protocolos abiertos existen varios como RIPv1, RIPv2 u OSPF entre otros, pero entre RIP y OSPF para redes de tamaño medio-grande es preferible, ya que OSPF permite una escalabilidad muy remarcable, entre otras características podemos decir que OSPF no tiene el problema de la limitación de los 15 saltos de RIP, además los tiempos de convergencia de OSPF son muchísimo mejores en todos los casos y además OSPF para el calculo de costes y rutas óptimas tiene en cuenta factores tales como el ancho de banda, lo cual permite elegir un camino supuestamente más lento si el camino que supuestamente es más rápido tiene menor ancho de banda, lo cual provocaría más lentitud de la transmisión. OSPF es uno de los protocolos que sin duda están preparados para las redes actuales. OSPF también considera la capacidad de escalabilidad de la red a través de la escalabilidad que permite un modelo jerárquico que es posible conseguir mediante la utilización de distintas áreas. OSPF utiliza la tecnología de estado del enlace, de forma opuesta a RIP que utiliza tecnología de vector distancia. Los enrutadores de estado de enlace mantienen una imagen común de la red e intercambian su información de enlaces desde un descubrimiento inicial hasta los cambios de la red. Los enrutadores de estado de enlace no realizan broadcast de sus rutas periódicamente como los enrutadores que utilizan vector distancia.

OSPF tiene las siguientes características.

- **Velocidad de convergencia**: En redes grandes, la convergencia utilizando RIP puede alargarse varios minutos, hasta que la tabla completa de enrutamiento de los enrutadores de la red se completa y se estabiliza. En OSPF el tiempo de convergencia es muchísimo menor ya que sólo se actualizan las rutas que han sido modificadas y estás son distribuidas por la red de forma rápida.

- **Soporte de VLSM**: RIPv1 es un protocolo de los denominados classful, y como tal no soporta VLMS, sin embargo tenemos que recordad que RIPv2 sí soporta VLMS.

- **Tamaño de la red**: En un entorno RIP una red con más de 15 saltos no es viable, ya que más de 15 saltos se considera inalcanzable. Sin embargo en un entorno de enrutamiento basado en OSPF no tenemos este tipo de limitación, ya que teóricamente no tenemos esta limitación de tamaño, aunque si seguimos las especificaciones de los fabricantes de enrutadores Cisco o Lucent Technologies nos recomiendan redes en las cuales no haya más de 400 enrutadores por área, obviamente pueden existir más áreas, pero la única limitación física, no debida al protocolo sería la de los 400 enrutadores por área. Esta característica hace de OSPF ideal para redes medianas y grandes.

- **Utilización de ancho de banda**: Si utilizamos RIP estamos realizando broadcast a la red de la tabla de enrutamiento completa cada 30 segundos. Esta característica puede ser especialmente problemática sobre lentos enlaces WAN. Sin embargo OSPF utiliza multicast y sólo envía actualizaciones cuando se produce un cambio en la red.

- **Selección de camino**: RIP selecciona el camino óptimo contando saltos, o distancia a otros enrutadores. Dentro de la elección de ruta óptima no entran en

consideración factores como el ancho de banda restante o los retardos en la red. Sin embargo OSPF utiliza una métrica basada en ancho de banda y retardos.

- **Agrupación de miembros**: RIP utiliza una topología plana en la cual todos los enrutadores forman parte de la misma red. Esta característica provoca que la comunicación entre enrutadores tenga que navegar por la totalidad de la red, de esta forma cada cambio en un enrutador individual afectaría al resto de los equipos de la red. Sin embargo con OSPF se introduce el concepto de "áreas", lo que permite la segmentación de la red en segmentos más pequeños. Al dividir la red en áreas se tiene que introducir el concepto de comunicación entre áreas, pero gracias a la división de la red los cambios producidos en un enrutador de un área no afectan a la totalidad de la red, sino que sólo afecta a los enrutadores de un área.

Ya que OSPF fue pensado y descrito para redes de un tamaño considerable al crear una red con más de 50 enrutadores hay que tener un cuidado especial con el diseño y la planificación de la red con tal de minimizar tráfico y el montante de intercambio de información de enrutamiento.

Como protocolo de estado del enlace, OSPF opera de forma distinta a los protocolos de vector distancia como podrían ser RIP.

La información proporcionada por OSPF a los vecinos no es la tabla de enrutamiento completa. Sin embargo, los enrutadores que utilizan OSPF le informan a sus vecinos sobre el estado de sus conexiones o enlaces. En otras palabras los enrutadores OSPF anuncian el estado de sus enlaces. Los enrutadores procesan esta información y generan la base de datos de estado del enlace, la cual es esencial para poder dibujar un esquema de quien está conectado con quien. Todos los enrutadores en una misma área tienen que tener una base de datos del enlace idéntica. Cada enrutador ejecuta independientemente el algoritmo SPF2, también conocido como algoritmo de Dijkstra, en la base de datos del enlace con tal de determinar las mejores rutas a los destinos. El algoritmo SPF añade el coste (el cual está normalmente basado en el ancho de banda) a cada uno de los enlaces entre el enrutador origen y el destino. Entonces el enrutador escoge el camino con coste más bajo y añade el camino a su tabla de enrutamiento también conocida como base de datos de *forwarding*.

Los enrutadores que utilizan OSPF mantienen información de sus vecinos y de sus bases de datos de adyacencia. Para simplificar el intercambio de información de enrutamiento sobre varios vecinos en la misma red, los enrutadores que ejecutan OSPF tienen que escoger el Enrutador Designado (DR3) y el Enrutador Designado de Backup (BDR4) para servir de punto central para la actualización de rutas.

Los enrutadores que ejecutan OSPF establecen relaciones, o estados, con sus vecinos para un intercambio de información de estado más eficiente. En contraste con los protocolos de vector distancia, como RIP, los cuales realizan broadcast o multicast de su tabla de enrutamiento completa por cada interfaz, esperando que los demás enrutadores la reciban. RIP por defecto envía cada 30 segundos sólo un único tipo de mensaje, su tabla completa de enrutamiento. Sin embargo, los enrutadores que ejecutan OSPF disponen de cinco tipos de paquetes distintos a enviar a sus vecinos para actualizar la información de estado del enlace. Estos cinco tipos de mensajes hacen de OSPF un protocolo adecuado para comunicaciones sofisticadas y complejas.
OSPF se relaciona con sus vecinos mediante siete estados distintos.

1.6.5.1.1 Topologías OSPF

En OSPF se pueden encontrar distintos tipos de topologías según el RFC2328, pero sin embargo ya se ha empezado a desarrollar soporte para otro tipo de topologías de forma propietaria.

1.6.5.1.1.1 Topología de Broadcast

Este tipo de topología se puede utilizar en entornos donde es posible que los enrutadores tengan en común una red de broadcast, como podría ser una red Ethernet, Token Ring o FDDI. En este tipo de topologías los enrutadores tienen en común una red que permite tráfico de multicast del DR con el resto de los enrutadores.

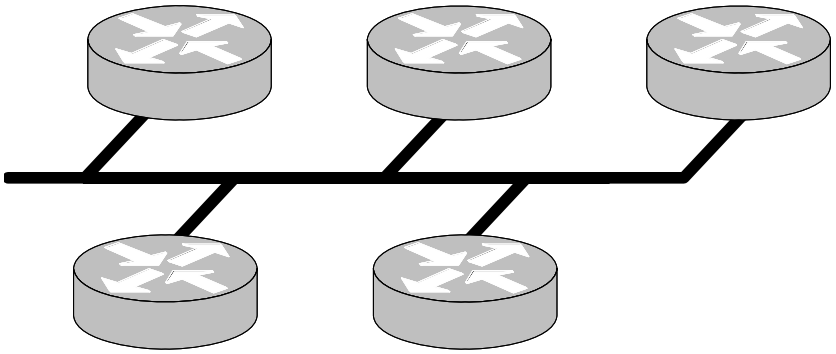


Figura 73. Topología de Broadcast

1.6.5.1.1.2 Topología Punto a Punto

Este tipo de topologías son las más simples, ya que en ella sólo entran dos enrutadores conectados de forma directa formando un único enlace.

Figura 74. Topología punto a punto

En este tipo de topologías no es necesario la elección de DB y BDR ya que sólo hay dos enrutadores.

1.6.5.1.1.3 Toplogía NBMA

En este tipo de topologías que no son de Broadcast, NBMA son las siglas de "NoBroadcast MultiAccess networks". En este tipo de topologíasb existe un problema adicional, ¿Cómo envíamos mensajes de multicast en este tipo de redes?, pues bien, esta pregunta sólo tiene una contestación posible, es decir, la contestación consiste en realizar una emulación de una red de broadcast.

La emulación de una red de broadcast en una red que no lo es sólo se puede hacer mediante la replicación de mensajes. Una red NBMA totalmente mallada, en la cual todos los enrutadores están conectados con todos los enrutadores tenemos que replicar un mensaje de multicast en muchos mensajes de unicast, es decir, en vez de enviar un único mensaje a la red a la dirección de multicast 224.0.0.5 tenemos que enviar el mismo mensaje por cada uno de los enlaces que tiene el enrutador con los demás enrutadores de la red, es decir, estamos realizando una topología que emula a una red de broadcast mediante un conjunto de redes punto a punto.

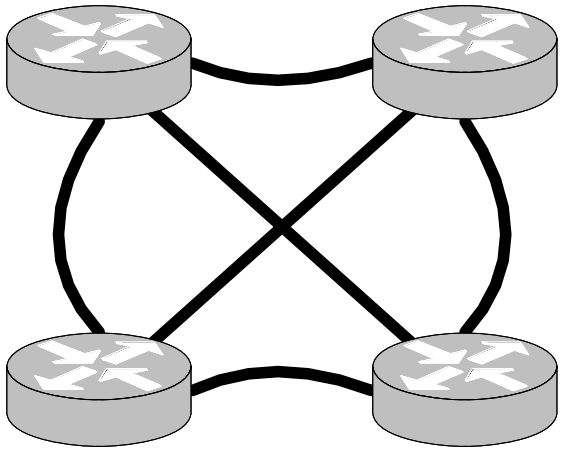


Figura 75. Topología NBMA totalmente mallada

1.6.5.1.2 Estados de OSPF

Para una comprensión más profunda de OSPF es necesario comprender las relaciones o estados que tienen entre si los enrutadores que utilizan OSPF.

- *Estado Down.* En el estado Down, el proceso OSPF no ha empezado a intercambiar información con ningún vecino. OSPF está esperando a entrar en el siguiente estado.

- *Estado INIT.* Los enrutadores que utilizan OSPF envían paquetes de tipo 1 (Hello) en intervalos regulares (por defecto 10 segundos en Zebra y en Cisco) para establecer relación con sus enrutadores vecinos, cuando un interfaz recibe su primer paquete Hello entonces decimos que el enrutador ha entrado en estado Init y está preparado para entrar en el siguiente estado.

- *Estado Two Way.* Utilizando paquetes Hello, cada enrutador OSPF intenta establecer una comunicación bidireccional con cada enrutador vecino que está ubicado en la misma red IP. Un enrutador entra en estado two-way en el momento que se ve en una de las actualizaciones de uno de sus vecinos.
El estado two-way es la relación más básica que pueden tener los enrutadores OSPF, pero la información de enrutamiento no se intercambia en este estado. Para aprender sobre enlaces de otros enrutadores el enrutador tiene que tener al menos una adyacencia completa.

- *Estado ExStart.* Técnicamente, cuando un enrutador y su vecino entran en estado ExStart, su conversación se caracteriza por una adyacencia, pero los enrutadores todavía no tienen una adyacencia completa. El estado ExStart se establece utilizando paquetes de tipo 25. Entre los dos enrutadores se utilizan paquetes hello para determinar cual de los dos es el maestro y cual es el esclavo en su relación y se intercambian paquetes de tipo 2.

- *Estado Exchange.* En el estado exchange se utilizan paquetes de tipo 2 para enviar al otro enrutador su información de estado del enlace. En otras palabras, los enrutadores describen sus bases de datos de estado del enlace al otro enrutador. Si alguna de las rutas no está en la base de datos del enlace del enrutador receptor de la información, este solicita una actualización completa, la cual se realiza en el estado Loading.

- *Estado Loading.* Después de que todas las bases de datos han sido descritas a cada enrutador, se tiene que solicitar una información que es más completa utilizando paquetes de tipo 36. Cuando un enrutador recibe un paquete de tipo 3, este responde con una actualización mediante un paquete de tipo 47. Los paquetes de tipo 4 describen la información de estado del enlace que es el corazón de los protocolos de enrutamiento de estado del enlace. Los paquetes de tipo 4 con respondidos con paquetes de tipo 58.

- *Adyacencia Completa.* Cuando termina el estado Loading, los enrutadores están en una adyacencia completa. Cada enrutador mantiene una lista de sus vecinos adyacentes, llamada base de datos de adyacencia. Es preciso no confundir la base de datos de adyacencia con la base de datos de estado del enlace o con la base de datos de forwarding.

Ya que la adyacencia es necesaria para que los enrutadores que utilizan OSPF puedan compartir su información de enrutamiento, un enrutador tiene que estar adyacente con al menos otro enrutador en la red IP a la que esté conectado. Si hay o no adyacencia depende del tipo de red que se esté utilizando, es decir, de qué tipo de red esté conectado los enrutadores.

Las interfaces de un enrutador que estén ejecutando OSPF tiene que reconocer tres tipos de redes: redes de broadcast (por ejemplo, ethernet), NBMA9 (por ejemplo, Trama Relay totalmente mallada) y redes punto a punto (sólo dos enrutadores). Un administrador de red podría configurar un cuarto tipo de red: red punto a multipunto.

El tipo de red en la que esté trabajando OSPF dictará el funcionamiento del protocolo, y este a su vez puede ser optimizado por el administrador de la red. Muchas redes se

definen como redes de multiacceso porque no es posible predecir cuantos enrutadores van a haber conectados.

1.6.5.1.3 Enrutadores OSPF

Debido a que en redes de multiacceso pueden existir un número significativo de enrutadores, OSPF utiliza un método para evitar la sobrecarga de información de enrutamiento en la red, de este modo la información se centraliza en dos enrutadores:

- **Enrutador Designado (DR, Designated Router)**: Para todas las redes de multiacceso IP se debe de elegir un DR. Este DR tiene dos funciones principales: Mantener adyacencia con todos los demás enrutadores de la red. Actuar de portavoz de todos los demás enrutadores de la red y anunciar los cambios a las otras redes, por supuesto es el encargado de mantener la información centralizada del estado de su red.

- **Enrutador Designado de Backup (BDR, Backup Designated Router)**: El DR puede representar un único punto de fallo, así que se elige un BDR para proporcionar tolerancia a fallos, es decir una redundancia. Así pues el BDR también tiene que ser adyacente a todos los demás enrutadores de la red y tiene que estar sincronizado con el DR para que en caso de caída del DR pueda este asumir la responsabilidad de la red. En redes punto a punto, en las cuales sólo existen dos nodos no tiene mucho sentido el que exista ni DR ni BDR, así que en este caso ambos enrutadores funcionan Peer-to-Peer.

- **Enrutadores Internos (IR)**: Los enrutadores internos tienen todos sus interfaces en una misma área. Todos los enrutadores de la mismo área tienen las mismas bases de datos de enlaces, es decir los enrutadores internos del mismo área al ejecutar el algoritmo SPF utilizan los mismos enrutadores como datos.

- **Enrutadores de Backbone (BR)**: Los enrutadores de backbone están situados en los límites del área de backbone y tienen al menos un interfaz conectado al área 0.

- **Enrutadores de enlace a Areas (ABR, Area Border Routers)**: Estos enrutadores como indica su nombre son los enrutadores que tienen enlaces a distintas áreas, estos enrutadores mantienen bases de datos del enlace separadas por áreas, es decir, tienen una base de datos independiente por área y ejecutan un SPF independiente por área.

- **Enrutadores de Frontera del Sistema Autónomo (ASBR, Automous System Boundary Routers)**: Estos enrutadores tienen al menos un interfaz con un AS (Sistema Autónomo) distinto. El AS distinto no tiene porque utilizar OSPF. Los ASBR distribuyen información no OSPF a la red OSPF y viceversa cuando es necesario.

Por supuesto un enrutador puede ser de varios tipos a la vez.

1.6.5.1.4 Tipos de LSAs

Los LSAs describen el estado de una red o de un enrutador. Esta descripción cubre el estado de todas las interfaces de los enrutadores y sus adyacencias. En OSPF utilizamos 4 tipos de LSAs:

- **Tipo 1**: Son llamados *router link*, estos LSAs describen el estado y el coste de los enlaces entre enrutadores de área. Estos LSAs sólo se propagan dentro de una misma área, no en todo el Sistema Autónomo.

- **Tipo 2**: Son llamados *network links*, estos LSAs describen todos los enrutadores que hay en una red en particular. Estos LSAs se propagan dentro del área que contiene la red.

- **Tipo 3 *I* 4**: Esos son los *summary links*. Estos LSAs se generan por los ABRs, y describen los enlaces entre los ABRs y los IRs del área local. Los *summary links* se propagan a través del área 0 o backbone a otras áreas a través de los ABRs del AS. Los LSAs de tipo 3 y de tipo 4 tiene diferencias.
Los LSAs de tipo 3 describen las rutas a las redes a través del AS y se envían por el área 0. Sin embargo los LSAs de tipo 4 describen la localización de los ASBR.

- **Tipo 5**: Son también conocidos como *external links*, los cuales se crean en los ASBRs. Estos LSAs describen las rutas a destinos fuera del AS. Estos LSAs van por las áreas estándar y por la backbone.
Existen dos tipos de external links:

    - External link type 1: Este se calcula añadiendo al coste externo el coste interno para alcanzar el destino.
    - External link type 2: Es el coste externo sin tener en cuenta el coste interno.

Tal y como se puede observar en la descripción de los tipos de área, ningún tipo de LSA atraviesa las áreas *totally stubby*.

1.6.5.1.5 Funcionamiento de OSPF

Cuando un enrutador arranca el proceso de enrutamiento OSPF en uno de sus interfaces, éste envía un paquete hello y continua enviando paquetes hello en intervalos regulares. En el nivel 3 del modelo de referencia OSI, los paquetes hello son enviados a la dirección de multicast 224.0.0.5. Esta dirección tiene el significado de “todos los enrutadores”. Los enrutadores que están ejecutando OSPF envían periódicamente paquetes hello para iniciar y mantener su adyacencia y para asegurarse que las adyacencias con sus vecinos no desaparecen. Los tiempos de actualización para el envío de paquetes hello son configurables, y por ejemplo fabricantes como Cisco envían por defecto paquetes hello en redes de broadcast cada 10 segundos, sin embargo en redes NBMA envían los paquetes cada 30 segundos, este sería el caso de redes Trama-Relay que utilizan OSPF como protocolo de enrutamiento. Para el inicio de OSPF se utiliza el protocolo *Hello* para realizar un intercambio inicial en el cual se procede a conocer a los vecinos de la red,

posteriormente se procede a descubrir las rutas, luego se eligen las rutas y posteriormente se mantienen la información de enrutamiento.

1.6.5.1.5.1 Fase 1: Intercambio de Información

En la fase de Intercambio de Información empezamos con los enrutadores caídos, en estado down, puesto que todavía no ha realizado ningún intercambio de información con ningún otro enrutador, en este momento el enrutador envía un mensaje de tipo Hello por cada uno de sus interfaces que utilicen OSPF aunque no conozca la identidad de ningún enrutador, incluyendo el DR, y esto lo hace enviando los paquetes Hello a la dirección de Multicast 224.0.0.5. Una vez hecho esto todos los vecinos reciben el paquete Hello del enrutador, entonces añaden este primer enrutador a la lista de sus vecinos, por lo que ya hemos llegado al estado init. En este punto todos los enrutadores vecinos del primero envían un paquete de respuesta al primero de los enrutadores, al igual que al resto de sus vecinos. Cuando el primer enrutador recibe información de enrutamiento en la que se puede ver a si mismo (el vecino lo conoce y lo añade a su tabla) entonces el primer enrutador entra en estado two way y todos los enrutadores en este estado estarán empezando a realizar una comunicación bidireccional. Una vez se ha establecido la comunicación bidireccional se produce la elección de DR y el BDR, esta elección se produce antes de que los enrutadores empiecen a intercambiar información sobre el estado del enlace (Recordemos que OSPF es un protocolo de estado de enlace). Como punto final de la fase de Intercambio de Información hemos de tener en cuenta que cada 10 segundos por defecto se asegura el funcionamiento de la conexión bidireccional enviando mensajes Hello.

1.6.5.1.5.2 Fase 2: Descubrimeinto de Rutas

Una vez que se tiene la comunicación bidireccional con el DR y el BDR entonces significa que ya se ha elegido el DR y el BDR, es decir, en este momento estamos en el estado exstart y los enrutadores ya están listos para descubrir la información sobre el estado del enlace de la red y empezar a crear sus bases de datos de estado del enlace, este proceso sólo pueden llevarlo aquellos enrutadores que hayan conseguido un estado de comunicación completo con el DR y el BDR, es decir, este proceso sólo pueden llevarlo a cabo los enrutadores que hayan establecido adyacencias con el DR y el BDR. Para realizar el descubrimiento de rutas los enrutadores adyacentes tienen que realizar el siguiente procedimiento:

1. Entre los dos enrutadores se decide cual tiene el ID más alto para decidir quien empieza el intercambio de información, esta negociación se realiza mediante paquetes Hello.
2. El Enrutador Designado (DR) envía un paquete DBD10 al enrutador Drother11, y este le envía al DR un DBD, entonces ambos enrutadores se envían un LSAck12, de esta manera ya han realizado el intercambio de información, pero todavía no han aprendido las rutas nuevas. El LSAck se envía como agradecimiento por la información sobre la base de datos. La Base de Datos no es la base de datos completa, sino sólo las cabeceras, esto se hace así para no inundar con tráfico inútil la red.

Una vez se ha realizado el intercambio de las cabeceras de la base de datos entonces si uno de los enrutadores implicados observa que le falta alguna entrada solicita la entrada completa mediante un mensaje LSR13 y el otro extremo le contesta con un LSU14 con la entrada completa de la red solicitada en el LSR. Para finalizar se intercambian mensajes LSAck y están en estado total.

1.6.5.1.5.3 Fase 3: Elección de Rutas

La elección de rutas óptimas es una tarea que OSPF desarrolla mediante el Algoritmo de Dijkstra o SPF15. OSPF ejecuta el algoritmo SPF para calcular la ruta o rutas óptimas para un destino en particular. Para poder ejecutar el algoritmo primero tiene que tener la Base de Datos de la Topología de la red al completo, tarea que ya ha realizado en los pasos anteriores. En cuanto OSPF ejecuta el algoritmo SPF tiene las rutas óptimas, teniendo en cuenta que ejecuta el algoritmo después de un tiempo de espera con tal de evitar que el posible flapping16 de las interfaces cause un recalculo del algoritmo innecesaria que produciría una carga importante de CPU en nuestro enrutador. OSPF por defecto según la RFC2328 permite hasta 6 rutas con igual coste hacia un único destino, esto nos permitiría la realización de balanceo de carga en caso que sea necesario.

1.7 Red Multiservicios

El desarrollo de las telecomunicaciones y de Internet ha hecho que tecnologías enfocadas a la unión de voz, video y datos, comiencen a ser una realidad tanto en el mundo de los negocios, del ocio así como de las investigaciones. Los problemas generados por la heterogeneidad del gran número de redes de telecomunicaciones existentes, están motivando el estudio de mecanismos que favorezcan la homogeneización de los medios de transporte de voz, video y datos.

La convergencia de las redes de telecomunicaciones actuales supone encontrar la tecnología que permita hacer convivir en la misma línea la voz, video y los datos. Esto obliga a establecer un modelo o sistema que permita "empaquetar" la voz y el video para que pueda ser transmitida junto con los datos. Además, existen otras razones por las que esta tendencia de convergencia está actualmente en proceso, por ejemplo, las redes de datos exceden las redes de voz, el ancho de banda para las redes de datos es más barato que para las redes de voz, el costo por uso y consolidación de la red son menores en las redes de datos que en la redes de voz, se puede manejar calidad de servicio (QoS), se manejan normas abiertas y existen avanzados procesadores digitales de señales (DSP) para las redes de datos. Hay nuevas aplicaciones integradas unificando mensajes de Fax, Pager, Celular, e-mail y voice mail. Existen una variedad de tecnologías que se están desarrollando actualmente, en el uso simultáneo de voz, video y datos

1.7.1 Voz sobre IP (VoIP)

La voz humana es una de las formas más efectivas de comunicación. Por lo tanto, no es sorpresa que los recientes avances en tecnología para el manejo de voz y la necesidad actual de desarrollo y crecimiento para permanecer a la vanguardia en el mundo de los

negocios han impulsado el desarrollo de Voz sobre el Protocolo de Internet (VoIP) como la unión confiable de la Telefonía y las redes de datos.

Muchos negocios, entre corporaciones grandes y pequeñas compañías de comercio electrónico, están a la espera de esta tecnología emergente que los llevara hacia una mayor eficiencia, productividad y costos menores. VoIP no solo reducirá la redundancia de gastos de red, permitirá la transferencia de información de una manera más eficiente entre: computadoras, computadora y teléfono, y computadora y fax. Mientras que los beneficios de la integración de las redes de datos y voz son numerosos, las modificaciones de la infraestructura de red son a menudo malentendidas. Esto es verdadero cuando consideramos el papel del cableado de datos en el ancho de banda administrado.

1.7.1.1 ¿Què es VoIP?

VoIP es un tipo de convergencia de red. Específicamente, es la unificación de voz y datos sobre una única infraestructura de red. La idea detrás de VoIP es convertir rápidamente las comunicaciones digitales y analógicas (como lo son las llamadas telefónicas y los faxes) en paquetes IP para poder ser enviados a través de una red en vez de enviarlos sobre una red separada de telefonía. Las señales de voz primero se digitalizan, posteriormente son divididas en paquetes de información y enviadas a través de la red IP.

El protocolo de Internet es el protocolo más usado en nuestros días en lo que a redes LAN se refiere, Su popularidad hace que IP sea un protocolo unificado para soluciones en telefonía. Las compañías que tienen infraestructura LAN/WAN donde trabaja IP, muy fácilmente pueden implementar VoIP. Buenas soluciones de telefonía interna en IP pueden escalarse desde el entorno LAN hacia la WAN a través de sistemas amplios utilizando los enlaces WAN.

Dado que IP es un protocolo no orientado a conexión normalmente trabaja en conjunto con el protocolo orientado a conexión TCP para asegurar y garantizar la entrega del servicio. Sin embargo, aunque este trabaja muy bien con los datos (cual paquete que no llega a su destino es retransmitido), este no puede trabajar con aplicaciones en tiempo real, porque cualquier letra recibida fuera de la secuencia en la estructura de una sentencia resultará en un mensaje mutilado.

Debido a esto, una nueva norma fue requerida para las aplicaciones en tiempo real como lo son la voz y el video, las cuales han aumentado en popularidad. La norma H.323 provee una unificación para las comunicaciones de audio, video y datos a través de redes basadas en IP. Atendiendo la norma H.323, los productos y aplicaciones multimedia de diferentes proveedores pueden interoperar a través de este tipo de redes, incluyendo Internet. La comparación entre la norma ITU H.323 y el modelo de referencia OSI se puede ver en la Figura 76.

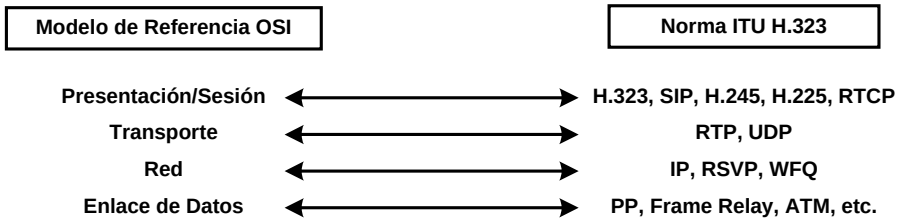


Figura 76. Comparación entre el Modelo de Referencia OSI y la norma ITU H.323.

VoIP usa la norma ITU H.323 en lugar del modelo de Regencia OSI, y aunque VoIP usa TCP para los canales de señalización, las aplicaciones de audio en tiempo real utilizan el RTP (Real Time Protocol). RTP usa al protocolo no orientado a conexión UDP como transporte ya que tiene un retraso menor que TCP y las retrasmisiones no son permitidas. VoIP es la implementación más popular de voz y su crecimiento prevalece gracias a las aplicaciones basadas en la norma H.323.

1.7.1.2 Componentes de un Sistema VoIP

Las tecnologías fundamentales implementadas con VoIP han sido caracterizadas, necesitamos considerar la implementación física, que son los componentes que harán que nuestro sistema funcione

1.7.1.2.1 Teléfono IP

El teléfono IP es un equipo que causa confusión entre la gente que usa los teléfonos tradicionales. Aunque el equipo se asemeja a un teléfono normal que es conectado a un puerto del PBX, el teléfono IP se conecta a la red Ethernet de la misma manera que se hace con una PC. Como el teléfono IP tiene una solo dirección MAC Ethernet (como la norma NIC en una PC de escritorio), después de la configuración inicial este puede ser conectado y usado en cualquier lugar de la red LAN. Algunos teléfonos IP poseen un Concentrador interno que permiten la conexión de cable LAN en el mismo teléfono con el cual podemos conectar a una PC.

Los teléfonos IP comúnmente requieren de una fuente de poder externa, pero algunos proveedores han solucionado este problema desarrollando Conmutadores que permiten que las fuentes de voltaje de corriente directa alimenten los equipos usando los cables que son utilizados en el UTP, esto elimina la necesidad de tener fuentes de poder externas en nuestro escritorio.

Es un hecho que no hay necesidad de un teléfono físico en la actualidad. Softphone es un software que simula un teléfono en tu PC. Con una tarjeta de sonido, un micrófono y unas bocinas en tu PC podemos tener toda la funcionalidad de un teléfono real mientras mantenemos una comunicación multimedia.

1.7.1.2.2 Conmutador LAN

Este tipo de Conmutador tiene la característica de minimizar los retrasos cuando es implementada esta Tecnología. Las conexiones de este Conmutador deberían ser solo utilizadas con teléfonos IP. Los equipos que comparten el medio como los concentradores no deberían ser usados con equipos que introduzcan retrasos inaceptables. También es importante que el Conmutador maneje QoS (como la norma 802.1p donde un número de bits en la tramade ethernet son usados para prioridad) para que los paquetes de voz puedan tener prioridad a través de la red LAN.

La redundancia es un punto importante que también debe ser considerado. En un ambiente donde solo existe VoIP, alguna falla en el Conmutador o en los enlaces entre los Conmutadores traería consigo la pérdida de la conectividad, con grandes consecuencias para la compañía. Por lo consiguiente la infraestructura de la LAN debe tener redundancia entre los equipos y en los enlaces utilizados.

1.7.1.2.3 Enrutador IP

Los enrutadores son utilizados para la transmisión de información entre los enlaces WAN de la compañía, comúnmente contratando conexiones de ISDN o Trama Relay. Cuando los paquetes de voz son enviados hacia esto enlaces es necesario incrementar el ancho de banda del enlace contratado o el CIR (Committed Information Rate) para que los enlaces Trama Relay puedan contener el tráfico. Si nosotros nos aseguramos de la prioridad dada a los paquetes de voz, entonces debemos estar seguros que nuestro enrutadores manejen QoS.

1.7.1.2.4 PBX IP

También conocido como la Unidad de Control de Servicio (SCU) o Administrador de llamadas, este equipo es el corazón de nuestro sistema VoIP y despliega todas las funciones de un PBX tradicional. Estas funciones incluyen conmutación y administración de llamadas, traslación de números telefónicos a direcciones IP, procesamiento de señales de voz, y establecimiento y administración de llamadas. También tiene aplicaciones de voz como correo de voz, autoatender y aplicaciones basadas en web. El PBX IP puede ser implementado con hardware o software. Algunos proveedores manejan software que pueden trabajar en plataformas como Windows NT, las implementaciones con hardware poseen un modulo procesador de llamadas, un gateway y usualmente se utilizan discos duros para habilitar el servicio de correo de voz.

1.7.1.2.5 Gateway PSNT

Este permite el traslado entre la red IP y la Red Telefónica Pública Conmutada (PSTN), en otras palabras, entre el dominio de los paquetes conmutados y el dominio de los circuitos conmutados. Esto es esencial debido a que es necesario enrutar las llamadas originadas en la red IP hacia la PSNT. Dado que los gateways pueden interoperar con los PBXs, esto significa que el equipo existente puede ser retenido para trabajar con el

sistema de telefonía IP. Los gateways pueden permanecer fuera de los equipos, ser módulos de los enrutadores o incorporarse con los PBXs IP.

1.7.1.2.6 Sistemas Integrados

La mayoría de los grandes proveedores ahora ofrecen sistemas de telefonía IP integrados, es un equipo modular que integra al PBX IP, al Gateway PSNT y al enrutador. Es una plataforma para correo de voz, auto asistente y aplicaciones de voz y datos basadas en la Web. Los discos duros son utilizados para dar la capacidad de correo de voz. Estos sistemas son usualmente implementados con teléfonos IP haciendo una proposición atractiva para los clientes que necesitan un paquete de soluciones para sus requerimientos de VoIP.

1.7.1.3 Beneficios de la Integración de Voz y Datos

VoIP elimina las redes redundantes y los recursos de red, simplifica la administración de la red y facilita la comunicación. Como consecuencia, las mayores ventajas de la Voz sobre IP son la reducción de costos y el incremento de productividad.

- ***Reducción de Redes Redundantes:*** Debido a que los típicos PBXs (Public Branch Exchanges) tienen altos costos de operación, VoIP resulta en un ahorro sustancial en la infraestructura de costos aún en un solo edificio.
- ***Evitar Costos de Tarifas Regulatorias***: el ambiente corporativo anticipa que la convergencia traerá ahorros en llamadas de larga distancia, especialmente en llamadas internacionales donde una parte considerable del costo deriva de los costos regulados. En muchos de los casos, estos sobrecargos no aplican en circuitos a través de los cuales se envían de datos. VoIP es una manera más barata de hacer llamadas telefónicas.
- ***Diversidad en el enrutamiento de las llamadas de voz:*** A pesar de un servicio telefónico muy confiable, las grandes compañías a menudo contratan varios circuitos a la compañía de telefonía local para actuar como un sistema de reserva. Sin embargo, estos circuitos son raramente utilizados y duplican el costo por mes que la compañía debe pagar por mantener esas líneas telefónicas de acceso. Con VoIP, si una falla ocurre en el circuito primario de un teléfono en una locación, la red de datos podría ser usada para enrutar llamadas temporalmente en los PBXs hacia otros lugares de la compañía. Esto elimina la necesidad de un circuito telefónico redundante, usando la red de datos de la compañía.
- ***Facilidad de altas, cambios y movimientos:*** Es costoso para una compañía mantener un área de trabajo que incluya conectividad de voz y datos, especialmente cuando existen movimientos de equipo de un escritorio a otro. Con DHCP (Dynamic Host Configuration Protocol, el cual habilita la asignación dinámica de direcciones IP para los equipos en la red), el movimiento de una PC de una LAN a otra es más simple debido a la autoconfiguración funcional. Sin embargo, el movimiento de una extensión telefónica de un escritorio a otro (o a otro edificio) no es tan simple, por lo general se requiere reconfigurar los sistemas de PBXs. Con el incremento de la popularidad de VoIP, un nuevo tipo de PBX y un teléfono IP ha entrado al mercado. Un teléfono IP puede autoconfigurarse por si mismo como un cliente de DHCP. Ahora solo se requiere de un simple jack de datos al lado del escritorio, y el teléfono IP puede actuar como un Concentrador o Conmutador que provee un puerto de datos para la PC del usuario. Una o

más PCs, o quizás un fax IP, pueden estar directamente conectados al teléfono IP y todos ellos pueden utilizar la red IP local. El movimiento de empleados de un escritorio a otro ahora es menos costoso.

- ***Costo de equipos IP menor:*** El empaquetado de voz pone a los equipos de datos en la red cerca de los puntos finales de la red, donde el equipo de empaquetado y conmutación muestra un desempeño mejor en cuanto a funcionamiento y es menos costoso con respecto a un equipo de conmutación. Con muchas compañías desarrollando nuevas características para los equipos IP, la razón costo/desempeño para estos equipos continuará mejorando. La tecnología de este tipo de equipos puede mantenerse al nivel en el incremento de la demanda para IP.
- ***Manipulación de Datos:*** Una sola conexión de red hacia el web (vía VoIP) también permite a Internet disponer de nuevas formas de comunicación como el *voice mail*: e-mail e imágenes de video en vez de usar una costosa y convencional línea telefónica. La información puede ser consultada y adquirida de diversas formas. La información basada en Internet (como lo es el e-mail y el comercio electrónico) pueden ser ahora consultada por teléfono usando comandos de voz. Una computadora de escritorio (además de recibir e-mails) puede ahora actuar como un teléfono de negocios y un fax. Por lo tanto, debido a VoIP, las organizaciones ahora reconocen el potencial de una interacción mas cercana con sus actuales y potenciales clientes.

1.7.1.4 Conversión de Voz a Datos

Para que una red basada en TCP/IP existente pueda rápidamente trabajar con trafico de VoIP, diversas modificaciones deben ser hechas a la red para que actúe como una red de circuitos conmutados.

Las redes de voz tradicionales se basan en circuitos conmutados. Estas redes usan un enlace dedicado de comunicaciones para cada llamada, con una taza de transferencia de 64 kbps. Sin embargo, los silencios consumen más de la mitad del promedio en tiempo de una llamada telefónica y si no se hacen llamadas, este ancho de banda no puede ser utilizado para otro tipo de tráfico. Este es un claro ejemplo de uso ineficiente del ancho de banda.

Sin embargo, esta ineficiencia es la que hace que las redes telefónicas sean confiables. Comparados con el sistema telefónico, una red de datos esta más propensa a experimentar problemas con le servidor u otros retrasos similares. De acuerdo con Lucent Technologies, los problemas telefónicos son raros porque el 80% de los problemas de la red de voz son solucionados sin la intervención del hombre. Esto es resultado del diseño de los circuitos conmutados en las redes telefónicas y el ancho de banda dedicado para cada línea. Desde que hay una cantidad fija de ancho de banda usada durante una llamada telefónica, los datos de voz nunca dejan de ser recibidos en secuencia hasta el fin de la conexión. Cuando los datos viajan a través de la red, esto son divididos y transmitidos a través de paquetes de información. Si estos paquetes se pierden, pueden ser transmitidos al final o fuera del orden debido a que tomaron caminos diferentes. Ahora, una de las consideraciones de diseño más importantes en la implementación de voz es la reducción del retraso. La retransmisión no es una opción con el flujo de tráfico de voz y video. Este tiene que transmitirse en tiempo real, si hay un retraso muy largo en la entrega de paquetes, el dato es irreconocible.

La transmisión secuencial y en tiempo real hacen de la administración del ancho de banda sea un factor crucial. Con VoIP, la infraestructura de la red de datos necesitara poder manejar más tráfico que antes.

La compresión de datos, el enrutamiento y el procesamiento son puntos de importancia.

Compresión: La tasa de transmisión para una llamada telefónica convencional es aproximadamente de 64 kbps, este de ancho de banda se considera excesivo, y es usualmente reducido por la entrega sobre una red de datos típica. Varias codificaciones y algoritmos de compresión están disponibles para reducir el consumo de ancho de banda hecho por una llamada telefónica. Estos mecanismos de compresión se encuentran usualmente en los gateways de VoIP y no en los Enrutadores y Conmutadores de la red de datos.

Calidad de Servicio de la Red: Una red TCP/IP debe tener mecanismos implementados para darle prioridad al tráfico IP sobre otros tipos de tráfico sobre la red (excepto otro tráfico de aplicaciones en tiempo real como lo es el video). El protocolo llamado *Resource Reservation Protocol* (RSVP) ha sido diseñado para reservar recursos a través de la red para las trasmisiones en tiempo real. Los mecanismos de Calidad de Servicio (QoS) con TCP/IP han sido también recientemente implementados por un número de vendedores de Enrutadores TCP/IP y Conmutadores. Las redes ATM y las redes Trama Relay tienen ya funcionalidad QoS implementada en su tecnología. Generalmente, los Enrutadores TCP/IP y los Conmutadores usan un sistema de prioridad en cola para almacenar paquetes que no sean de VoIP y enviarlos hasta que todos lo paquetes de VoIP hayan sido transferidos hacia el siguiente elemento de red. Los paquetes grandes de IP (no de VoIP) son almacenados al lado para poder enviar los paquetes de VoIP a tiempo. Otro mecanismo predice tiempos de congestión sobre el enlace de red y utiliza el ancho de banda demandado por las aplicaciones que no son realizadas en tiempo real.

Precedencia de los paquetes IP: debe ser fijada en el límite de la red, dándole al tráfico de VoIP la más alta precedencia posible. Las redes de datos con otros protocolos diferentes a TCP/IP no son bien vistas por VoIP por que es más difícil darle prioridad de tráfico cuando los paquetes no son de TCP/IP. Cuando sea posible, todo el tráfico de los Bridges debería ser segregado desde los enlaces WAN de TCP/IP donde fluirá el tráfico VoIP. El Bridging sobre cualquier clase de área amplia obstaculizará la puesta en práctica de implementaciones de QoS para TCP/IP.

Weighted Fair Queuing: WFQ es un mecanismo de almacenamiento para paquetes de TCP/IP, clasificándolos basándose en diferentes criterios y después entregándolos basándose en su precedencia IP. Las clasificaciones disponibles son: dirección fuente y destino, protocolo e identificador de sesión. Durante el proceso de decolamiento, a los paquetes se les da privilegio basándose en los tres bits de precendencia IP en el encabezado de los paquetes IP.

Procesamiento de los datos de Voz: Ya que en los portales de voz o sitios basados en VoIP, el reconocimiento de voz es procesado en el servidor de red y no por el teléfono. Esto permite que el sistema soporte millones de llamadas y que también reconozca la diversidad de clientes que puedan hacer petición para obtener la información. La VoIP es dirigida por gateway de voz hacia los hosts con el hardware y software necesario para la Telefonía en Internet. El gateway es implementado entre la Red Telefónica Pública Conmutada (PSTN) y el Protocolo de Internet en la Red. El Gateway ayuda a través de

señales a las redes de teléfonos, recepción de números telefónicos, conversación entre números telefónicos y el direccionamiento IP en la red IP y la conversación de voz en paquetes.

Mientras que estás aplicaciones reducen considerablemente los problemas de tráfico de datos, que da en duda que estas aplicaciones incrementaran la demanda de ancho de banda.

1.7.2 Videoconferencia

Desde los años 80, la comunicación video corporativa ha ayudado a la gente situada en diversas ciudades para comunicarse más con eficacia. Las soluciones de primera generación fueron basadas sobre la Unión Internacional de Telecomunicaciones (ITU) norma H.320 definiendo la Red Digital de Servicios Integrados (RDSI, ISDN por sus siglas en inglés) Videoconferencia basada en conexión. Las soluciones de segunda generación llevaron la Videoconferencia a las computadoras, pero aún dependía de la red ISDN y los dispositivos codificadores (CODEC) eran muy costosos. Para mediados de los 90's, las soluciones de tercera generación basadas en redes LAN comenzaron un viaje ubicuo de aplicaciones de Videoconferencia accesible para computadoras de escritorio, pero hasta hace poco permanecían protocolos propietarios, con implementación y control difíciles, y muy caras. La ausencia de normas tiene muchas limitantes de extensión, desarrollo e incompatibilidad entre diferentes soluciones de vendedores.

Las nuevas normas H.323 y H.324 permiten el establecimiento de una red y aplicaciones de vendedores para soportar más comunicación manejable y comparable de Videoconferencia. La norma H.323 define la Videoconferencia sobre redes LAN, y permite la interoperabilidad entre distintos fabricantes. La norma H.324 define la Videoconferencia usando líneas de la Plain Old Telephone System (POTS).

1.7.2.1 Norma H.323

La norma H.323 es una extensión lógica de la norma H.320 para habilitar Intranets de corporativos y redes de conmutación de paquetes, para transportar multimedia y Videoconferencia. La norma H.323 atraviesa los requisitos técnicos para los servicios visuales de banda estrecha de la telefonía que incluyen un o más LANs. Las recomendaciones cubren dispositivos IP que participan y controlan sesiones y elementos H.323 que interactúan con la red de circuitos conmutados (SCN, Switched Circuit Network). La norma H.323 no incluye la LAN en si misma, ni la capa de transporte que interconectan los segmentos LAN.

En común con otras normas de la teleconferencia de multimedia de la ITU, la implementación H.323 aplica para sesiones punto a punto y para sesiones multipunto. La recomendación H.323 permite Videoconferencias multipunto a través de una variedad de métodos o configuraciones. La recomendación permite tecnologías centralizadas y descentralizadas de la Videoconferencia.

La ITU ha ratificado estos componentes del Core:

- H.225: Especifica los mensajes para el control de llamadas incluyendo la señalización, registros y admisión, y paquetización/sincronización de medios streams.
- H.245: Especifica los mensajes para abrir y cerrar los canales para medios streams, y otros comandos, peticiones e indicaciones.
- H.261: Codificación de video para los servicios audio-visuales en P x 64 kbps
- H.263: Especifica una nueva codificación de video para la POTS (Plain Old Telephone System).
- G.711: Codificación de audio, 3.1 kHz a 48, 58 y 64 kbps (telefonía clásica).
- G.722: Codificación de audio, 7 kHz a 48, 58 y 64 kbps.
- G.728: Codificación de audio, 3.1 kHz a 16 kbps.
- G.723: Codificación de audio, para modos de 5.3 a 6.3 kbps.
- G.729: Codificación de audio.

1.7.2.1.1 Audio H.323

Las señales de audio contienen digitalización y compresión del sonido (usualmente un discurso). H.323 soporta normas de algoritmos de codificación de audio aprobadas por la ITU, incluyendo G.711 para discursos, el cual transmite a 56 ó 64 kbps. Soporta otras normas para voz (G.722, G.723, G.728, G.729) son opcionales, cada uno con diferentes calidades de audio, tasas de transferencia, delay (retardo) en la señal y procesamiento en el equipo.

1.7.2.1.2 Video H.323

Las capacidades de video son opcionales. Las terminales H.323 deben soportar la codificación H.261, con opción de soportar la codificación H.263. La transmisión no es mejor que la seleccionada durante un proceso de intercambio de capacidades durante la disposición de la llamada. H.261 y H.263 cualquiera de los dos soporta QCIF, comunicación entre diferentes terminales es posible. (Ver tabla 42).

Formato:	Tamaño de Imagen:	H.261	H.263
Sub-QCIF	128x96	opcional	requerido
QCIF	176x144	requerido	requerido
CIF	352x288	opcional	opcional
4CIF	702x576	N/A	opcional
16CIF	1408x1152	N/A	opcional

Tabla 42. Formato de Video.

La norma H.261 provee algunas compatibilidades a través de muchas recomendaciones de la ITU, y son usadas con canales de comunicaciones múltiplos de 64 kbps. H.261 codifica completamente las tramas iniciales, después sólo codifica las diferencias entre la tramainicial y la tramasubsecuente para la transmisión mínima de paquetes. La compensación mejora la calidad de la imagen y es una opción.

La norma H.263 es actualizable y compatible a la norma H.261. Este realiza significativamente una mejor calidad del video usando una técnica de estimación del movimiento, predicción de Tramas, y optimización por una tabla de codificación Huffman

para transmisiones de baja transferencia. La norma H.263 define 5 normas para el formato de video como se muestra en la tabla 41.

1.7.2.1.3 Datos H.323

La recomendación H.323 provee secuencias de datos opcionales en videoconferencias. Un sistema H.323 soporta datos a través de las capacidades de T.120 en los clientes y las MCU's. Las MCU's mezclan y controlan las secuencias de datos. La norma T.120 proporciona interoperabilidad en aplicaciones, red y en niveles de transporte en videoconferencias punto a punto, y en videoconferencias punto multipunto para los datos.

1.7.2.1.4 Señalización

H.323 usa solo un puerto muy conocido, para señalización Q.931. Puertos o sockets usados para señalización H.245, audio, video o canales de datos son negociados dinámicamente entre puntos finales. El uso de puertos dinámicos hace difícil la implementación de seguridad, políticas y traffic shaping.

La conferencia de datos H.323 usa comunicaciones fiables y comunicaciones inestables. Transporte fiable para señales de control y datos, porque las señales deben de ser recibidas en orden propio y no pueden ser perdidos. El transporte inestable es usado para streams de audio y video, los cuales son sensitivos al tiempo.
Retardo en paquetes de audio y video son tirados. Consecuentemente, TCP es aplicado para el canal de control H.245, el canal de datos T.120, y los canales de señalización, mientras los UDP's son aplicados para audio, video, y canales RAS.

1.7.2.1.5 Seguridad

Desde que las aplicaciones tienden a H.323 usan puertos asignados dinámicamente para audio, video y canales de datos, un firewall debe ser cualquiera de las dos cosas, habilitar H.323 con un Proxy, o estar dispuesto a identificar para control del canal para determinar cual puerto dinámico está en uso por las sesiones H.323, y permite el tráfico con tal de que el canal de control este activo.

1.7.2.1.6 Despliegue de Componentes H.323

La recomendación de la ITU H.323 describe los componentes de un sistema obediente H.323. Los componentes de una solución H.323 quizá incluye, pero no está limitada a terminales, Gateways, Gatekeepers, Controladores Multipunto (*multipoint controllers, MCs*), Procesadores Multipunto (*multipoint processors, MPs*), y Unidades de Control Multipunto (*multipoint control units, MCUs*). Otros componentes tratan el despliegue sobre las redes IP que tienen mecanismos de calidad de servicio (QoS), y elementos de seguridad como Proxies y Firewalls. Esta parte describe el papel de cada elemento en un sistema H.323 como parte de una red end-to-end.

1.7.2.1.6.1 Terminal

Una terminal H.323 es un punto final en la red de área local habilitada en tiempo real, con comunicación bidireccional ya sea con otra terminal H.323, un gateway o una MCU. La comunicación incluye información de control, indicaciones, audio, video y/o datos entre terminales. H.323 especifica el modo de operación para cada tipo de terminal. Ejemplos de terminales H.323 bajo desarrollo están teléfonos de Internet, terminales de audio conferencia y aplicaciones de videoconferencia de cualquier configuración.

Todas las terminales H.323 deben de soportar estas características:

1. H.245, una compleja norma para la negociar el uso del canal y capacidades,
2. Q.931, una norma para la señalización y configuración,
3. Registro/Admission/Status, RAS (Registro/Admisión/Estado), un protocolo para comunicarse con gatekeepers,
4. Soporte RTP/RTCP, para secuencias de paquetes de audio y video.

Las terminales H.323 opcionalmente, pueden soportar estas características:

- Codificadores de vides (*Video Codecs*),
- T.120 protocolo de datos de conferencia
- Capacidades de MCU
- Gateways

La figura 77 ilustra la interoperabilidad de diferentes tipos de terminales H.323.

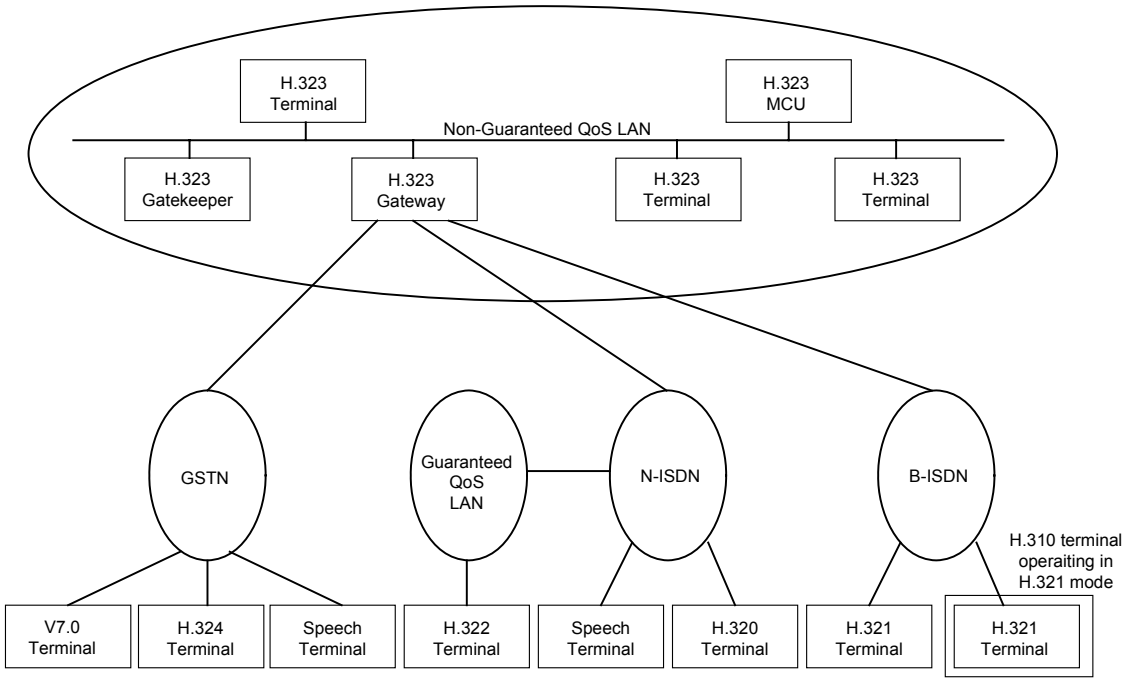


Figura 77. Interoperabilidad de diferentes tipos de terminales H.323.

Nota: Un gateway puede soportar una o más conexiones GSTN, N-ISDN y/o B-ISDN.

1.7.2.1.6.2 Gateway

Un gateway es una opción elemental en sistemas H.323, y es un punto final en la LAN que provee en tiempo real, dos vías de comunicación entre terminales H.323 o otros gateways sobre la LAN y otras terminales ITU en la WAN, usando los protocolos H.245 y Q.931. Los gateways no son requeridos cuando no hay conexión hacia otras redes.

Los gateways son encontrados donde los administradores de red necesitan para:

- Establecer enlaces con terminales PSTN analógicas,
- Establecer enlaces con terminales remotas que tienden a H.320 sobre ISDN,
- Establecer enlaces con terminales remotas que tienden a H.324 sobre redes PSTN,
- En general, un gateway refleja las características de un punto final en la LAN para un punto final SCN, y viceversa. Los gateways pueden transladar entre conferencias H.323 en puntos finales y tiendan a terminales. Esta función incluye translación entre formatos (por ejemplo, H.225 a H.221), o entre procedimientos de comunicación (por ejemplo, H.245 a H.242).

Los gateways también transladan entre codificadores de audio y video, y desempeñan la configuración de la llamada y limpian en ambos lados de la conexión LAN y los circuitos de la red de conmutación. Propiamente los gateways H.323 configurados pueden también soportar terminales que cumplan con las normas H.310, H.321, H.322 y V.70. La figura 78 ilustra un gateway H.323/H.320.

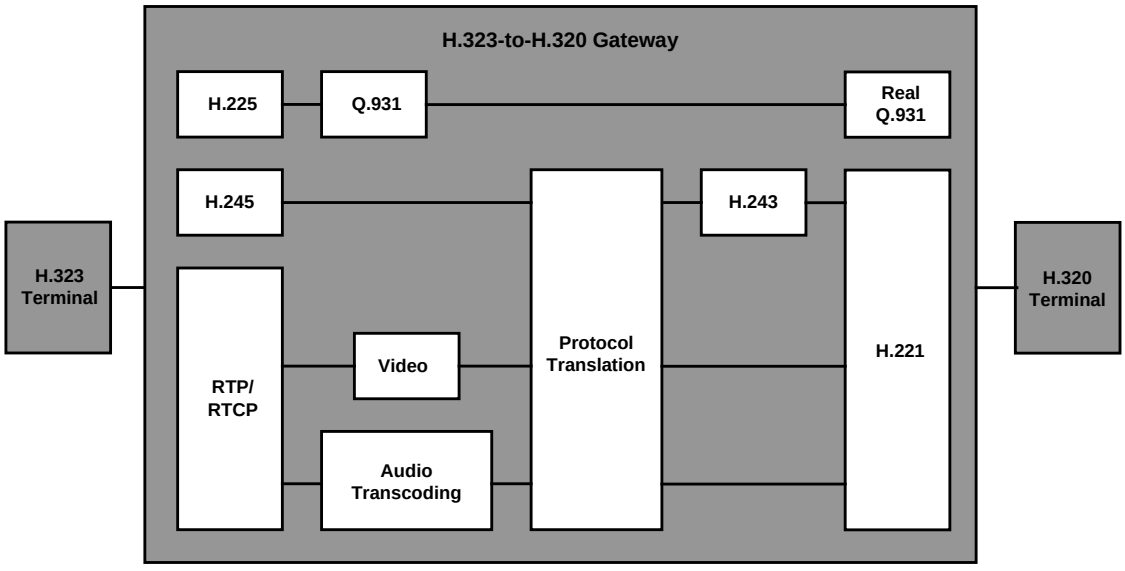


Figura 78. Gateway H.323/H.320.

1.7.2.1.6.3 Gatekeeper

También un componente opcional, los gatekeepers proveen llamadas de control de servicios para puntos finales H.323. Uno o más gatekeepers pueden ser desplegados, y son separados lógicamente por los puntos terminales. Mientras las normas de comunicación de gatekeepers a gatekeepers no están establecidas, la implementación física puede coexistir con una terminal, un MCU, un gateway, un MC u otros dispositivos LAN que no son H.323.

Los gatekeepers pueden proveer estos servicios:

1. Translación de dirección- Realiza la dirección alias para transportar la dirección de translación. Los gatekeepers usan típicamente una tabla de translación actualizada usando mensajes de registro (como se describe después), aunque permiten otros métodos de actualización de tablas.
2. Control de admisión- Autoriza el acceso a la LAN usando mensajes ARQ/ACF/ARJ/H225.0, basado en la autorización de la llamada, ancho de banda u otros criterios de configuración dados por el fabricante. Esto también puede ser una función nula que admite todas las peticiones sin filtrarlas.
3. Control del ancho de banda- Soporta mensajes BRQ/BRJ/BCF basados en la administración del ancho de banda. Esto también puede ser una función nula que admite todas las peticiones para cambios del ancho de banda.
4. Zona de administración- Provee funciones para registrar terminales, MCU's, y gateways.

1.7.2.1.6.4 Controlador Multipunto

Un MC es una entidad de H.323 basada en la LAN que controla tres o más terminales participando en conferencias multipunto. También puede controlar una conferencia punto a punto que se puede desarrollar en una conferencia multipunto. Una MC provee capacidades de negociación con todas las terminales para establecer niveles comunes de comunicación. También pueden controlar recursos de videoconferencias como video multicast. Una MC no mezcla o no conmuta audio, video y datos.

Una MC puede ser localizada dentro de un gatekeeper, gateway, terminal, o MCU. H.323 limita las arquitecturas de la conferencia para una MC por una conferencia multipunto. Con las soluciones de hoy, si una conferencia que tiene más de 10-20 participantes, los usuarios pueden encontrar un desempeño satisfactorio.

1.7.2.1.6.5 Procesador Multipunto

Un MP es una entidad H.323 basada en la LAN que procesa centralmente audio, video, y/o streams de datos en una conferencia multipunto. El MP mezcla, conmuta, y desempeña otros procesos para streams controlados por una MC. Puede procesar uno o muchos streams dependiendo del tipo de conferencia que está soportando.

1.7.2.1.6.6 Unidad de Control Multipunto

Una MCU soporta conferencias multipunto entre tres o más puntos finales. Como está definido por H.323, una MCU consiste de una MC requerida y una MP's opcional. Una MCU típica soporta conferencias multipunto centralizadas, consiste de una unidad de MC y una MP que soporta audio, video y streams de datos.

Para volver a llamar, la recomendación H.323 permite que cualquiera de las dos configuraciones de conferencias, centralizadas y descentralizadas, una MCU es requerida para la primera, mientras que para la segunda, puede ser administrada con tecnologías multicast.

Una MCU facilita las conferencias multipunto centralizadas, donde todas las terminales envían streams de audio, video, datos y control a la MCU en una conexión punto a punto. El MC desempeña una porción de H.245 de la negociaciones entre terminales para determinar las capacidades comunes de procesamiento para audio y video. También el MC controla recursos de las conferencias para determinar cuales streams de audio y video son multicast. La porción de negociaciones del MC no se ocupa directamente de estos setreams. La porción de negociaciones del MP toma cuidado del mezclado, la conmutación, y el procesamiento de streams de audio, video y datos. El MP también puede convertir entre diferentes codecs y tasas de transmisión, y puede usar algunas tecnologías multicast para distribuir streams de video procesado.

Las conferencias multipunto descentralizadas usan tecnologías multicast, relegando la MCU a un menor papel. Las terminales participantes usan multicasting para enviar los streams de audio y video para cada terminal sin la MCU. El control de datos y la información del canal de H.245 aún pasan a través del MCU. La porción del MP puede proveer la selección del video y la mezcla del audio en una conferencia multipunto descentralizada.

Las terminales receptoras procesan múltiples entradas de streams de audio y video. También las terminales usan canales de control H.245 para indicar a la MCU el número de streams simultáneos de audio y video que ellos pueden decodificar. Las limitaciones de una sola terminal no limita el número de streams simultáneos de audio o video que están en multicast entre los participantes.

Las conferencias multipunto híbridas usan una combinación de características centralizadas y descentralizadas. Las señales H.245 y cualquiera de los dos streams de audio o video son procesados por la MCU vía mensajes punto a punto. La permanencia de señales de audio y video es transmitida a las terminales participantes vía tecnologías multicast.

En una conferencia multipunto mixta, algunas terminales están centralizadas y otras están descentralizadas. El MCU sirve como bridge entre dos tipos de terminales. Las terminales son transparentes del bridging de la MCU.

1.7.3 Streaming

La tecnología de Streaming se utiliza para aligerar la descarga y ejecución de audio y vídeo en la Web, ya que permite escuchar y visualizar los archivos mientras se están descargando.

Si no utilizamos Streaming, para mostrar un contenido multimedia en la red, tenemos que descargar primero el archivo entero en nuestra computadora (PC) y más tarde ejecutarlo, para finalmente ver y oír lo que el archivo contenía. Sin embargo, el Streaming permite que esta tarea se realice de una manera más rápida y que podamos ver y escuchar su contenido durante la descarga.

El Streaming funciona de la siguiente manera. Primero nuestra PC (el cliente) se conecta con el servidor y éste le empieza a mandar el fichero. El cliente comienza a recibir el fichero y construye un buffer donde empieza a guardar la información. Cuando se ha llenado el buffer con una pequeña parte del archivo, el cliente lo empieza a mostrar y a la vez continúa con la descarga. El sistema está sincronizado para que el archivo se pueda ver mientras que el archivo se descarga, de modo que cuando el archivo acaba de descargarse el fichero también ha acabado de visualizarse. Si en algún momento la conexión sufre descensos de velocidad se utiliza la información que hay en el buffer, de modo que se puede aguantar un poco ese descenso. Si la comunicación se corta demasiado tiempo, el buffer se vacía y la ejecución el archivo se cortara también hasta que se restaurase la señal.

1.7.3.1 Elementos

Para realizar el streaming, se necesitan básicamente cuatro elementos:

1. Contenido digitalizado,
2. Un servidor de streaming,
3. Un programa de streaming,
4. Acceso a Internet (ISP).

1.7.3.1.1 Contenido Digitalizado

El material que se tiene pensado publicar vía Streaming, debe estar digitalizado en un formato que el programa de Streaming entienda, o también, se puede contar con una tarjeta capturadota de video para material que aun no este digitalizado o que sea material en vivo (Encoder).

1.7.3.1.2 Servidor Streaming

En principio no es necesario contar con un servidor especial para colocar archivos de audio o vídeo con descarga Streaming en el Web. Cualquier servidor normal puede mandar la información y es el cliente el que se encarga de procesarla para poder mostrarla a medida que la va recibiendo.

Sin embargo, existen servidores especiales preparados para transmitir Streaming. Aunque en muchas ocasiones no es necesario utilizarlos nos pueden ofrecer importantes prestaciones como mandar un archivo de mayor o menor calidad dependiendo de la velocidad de nuestra línea.

En determinados casos, como la puesta en marcha de una radio o la transmisión de un evento en directo, si que será imprescindible contar con un servidor de Streaming al que mandaremos la señal y con ella, la enviará a todos los clientes a medida que la va recibiendo.

1.7.3.1.3 Programa Streaming

Estos programas se necesitan para convertir los archivos de audio y video en un formato que con un programa cliente el usuario final es capaz de reproducirlo. Es lo que hacen programas como el Real Player o el Windows Media Player, programas que se instalan como plug-ins en los navegadores para recibir y mostrar contenidos multimedia por Streaming.

Para convertir los archivos de audio y vídeo al formato de cada programa de Streaming se utilizan unos programas especiales. Por ejemplo, el programa para convertir al formato que lee el Real Player se llama Real Producer.

1.7.3.1.4 Acceso a Internet (ISP)

Para poner en marcha el Streaming, es indispensable que en la parte donde se encuentra el servidor de Streaming se tenga un ancho de banda que depende del número de usuarios que acceden al servicio, y además, de la calidad del video y audio que queremos para nuestros usuarios. Este acceso a Internet lo proporcionan los ISP's, dependiendo del ISP será el medio físico de la conexión.

A continuación se muestra un diagrama del funcionamiento del Streaming, en la figura 79:

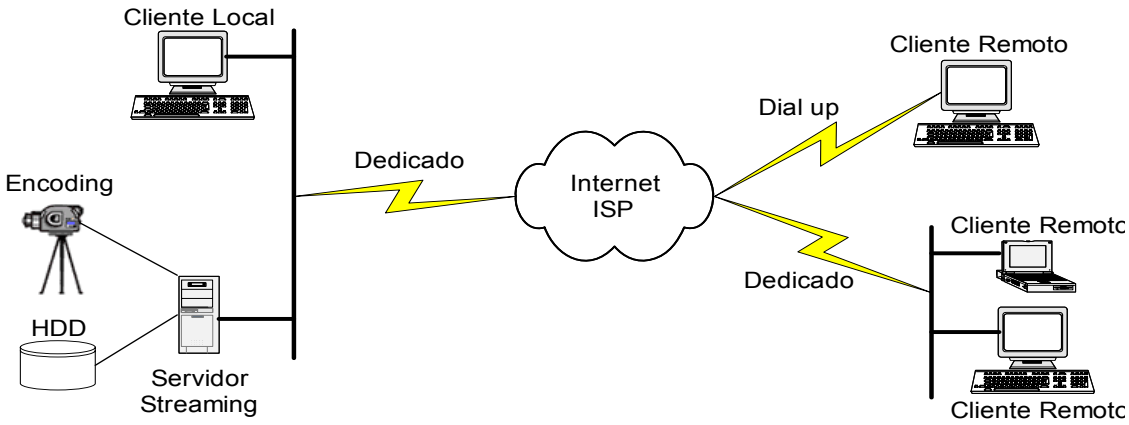


Figura 79. Funcionamiento del Streaming.

2. Diseño de Topología

2.1 Modelo de Diseño Jerárquico

Los Modelos Jerárquicos permiten el diseño de redes basándose en capas ya establecidas. Para entender la importancia del diseño basado en capas, se debe considerar el Modelo de Referencia OSI, el cual es un modelo de siete capas utilizado para implementar la comunicación entre hosts. Usando capas, el Modelo OSI simplifica las tareas requeridas por dos hosts para poder comunicarse. Los Modelos Jerárquicos para el diseño de redes también usan capas para simplificar las tareas requeridas para el diseño de una red. Cada capa se encarga de funciones específicas, permitiendo la elección de los sistemas y características correctos para cada capa.

2.1.1 Beneficios

Los diseños de red LAN tienden a seguir una de la dos estrategias generales de diseño: Malla y Jerárquica. En la estructura de Malla la topología de red es plana; todos los enrutadores desempeñan esencialmente las mismas funciones y usualmente no hay una definición clara de donde se realizan las funciones. El crecimiento de la red tiende a ser casual y arbitrario. En una estructura jerárquica la red es organizada en capas, las cuales tienen una o más funciones específicas. Los beneficios que presenta la utilización de un modelo jerárquico son los siguientes:

- *Escalabilidad:* Las redes que siguen el modelo jerárquico pueden crecer mucho más grandes sin sacrificar flexibilidad y control, debido a que la funcionalidad esta bien estructurada y los problemas potenciales pueden ser reconocidos más fácilmente. Un ejemplo de un diseño de red a gran escala utilizando el modelo jerárquico es la Red Telefónica Pública Conmutada (PSTN).
- *Fácil Implementación:* EL diseño jerárquico asigna funciones claras para cada capa, haciendo la implementación de red mucho más sencilla.
- *Fácil Localización de Fallas:* Debido a que las funciones de cada capa están bien definidas, el aislamiento de los problemas en la red es menos complicado. La segmentación temporal de la red para reducir el alcance de algún problema es mucho más sencillo también.
- *Fácil Predicción:* Usando un modelo de capas funcionales el comportamiento de una red es mucho más predecible, lo que nos ayuda a tener un plan de crecimiento considerablemente más sencillo y fácil de implementar, esta aproximación de diseño también nos permite facilidad en el modelo de desempeño de red para propósitos analíticos.
- *Soporte de Protocolos:* La mezcla de aplicaciones y protocolos actuales y futuros será mucho más fácil en redes que siguen los principios del diseño jerárquico debido a que la infraestructura actual ya esta lógicamente organizada.
- *Flexibilidad:* Todos los beneficios mencionados anteriormente contribuyen para tener una mayor flexibilidad de la red.

2.1.2 Componentes del Modelo de Tres Capas

El modelo de diseño jerárquico de red consta de tres capas:

- El Backbone provee el transporte óptimo entre sitios, utilizando enrutadores y switches optimizados para obtener buena disponibilidad y funcionamiento en la red interna.
- La Capa de Distribución que provee conectividad basada en implementación de Políticas, por medio de enrutadores y switches.
- La Capa de Acceso que provee a los grupos de trabajo y sus usuarios acceso a la red, mediante concentradores, switches y otros dispositivos.

Cada capa provee funcionalidad necesaria para la red. Las capas no deben ser implementadas como entidades físicas distintas. Cada capa puede ser implementada mediante enrutadores o switches, representándose por el medio físico o combinada en una simple caja. Alguna capa en particular puede ser omitida en el modelo, pero para un desempeño óptimo, la jerarquía se debe mantener.

2.1.2.1 Backbone

Es la capa de alta velocidad de la red interna, la cual es de suma importancia para habilitar y mantener un buen enlace de comunicación en el corporativo. Debido a esto la conectividad es crítica y debe ser diseñada con componentes redundantes. Esta capa debe tener una alta confiabilidad y adaptarse a los cambios rápidamente

2.1.2.1.1 Funciones del Backbone

La función primordial del Backbone es proveer un transporte óptimo entre sitios. El Backbone es, por lo tanto, usualmente implementado como una WAN. La característica de área amplia del enlace puede indicar la necesidad de trayectorias redundantes, debido a que la red puede provocar interrupciones de circuito individuales y continuar funcionando. El balanceo de carga y la convergencia rápida de los protocolos de enrutamiento pueden ser características importantes de diseño. Debido a las tarifas del proveedor, el uso eficiente del ancho de banda en el Backbone es siempre una preocupación.

Cuando se configuran enrutadores en esta capa, las características que optimizan el enrutamiento de paquetes deben ser implementadas. Se debe evitar el uso de filtros de paquetes u otras características que puedan retrasar la entrega de paquetes. Esta capa tiene que optimizarse para un estado de latencia bajo y una buena flexibilidad.

El Backbone debe tener un diámetro limitado y constante. Los enrutadores o switches de la capa de Distribución y los clientes de la red LAN pueden ser agregados al modelo sin considerar este diámetro. La limitación del diámetro de esta capa proporciona funcionamiento y facilidad para la localización de fallas.

Para los clientes que necesitan conectarse con otras empresas vía extranet o Internet, la topología del Backbone puede contener uno o más enlaces hacia redes externas. Los

administradores de la red corporativa tienen que planear sus propias extranet o conexiones a Internet, en vez de dejar este trabajo a los administradores locales o de alguna rama corporativa. Centralizar estas funciones en el Backbone ayuda a reducir la complejidad de problemas de enrutamiento potenciales y es esencial para reducir los problemas de seguridad.

El Backbone debe, en resumen, realizar las siguientes funciones:

- Ofrecer gran confiabilidad,
- Proveer redundancia,
- Proveer tolerancia a fallas,
- Adaptación a cambios rápidamente,
- Ofrecer bajo estado de latencia y buena flexibilidad,
- Evitar la lenta manipulación de paquetes causada por el filtrado u otros procesos, y
- Tener un diámetro limitado y consistente.

2.1.2.2 Capa de Distribución

La Capa de Distribución es el punto de demarcación entre las capas de Acceso y el Backbone de la red.

2.1.2.2.1 Funciones de la Capa de Distribución

La capa de Distribución debe incluir el Backbone del campus con todos sus enrutadores respectivos. Debido a que las Políticas de Administración de Red son implementadas en este nivel, podemos decir que la Capa de Distribución provee una conectividad basada en políticas. Estas políticas incluyen las convenciones de nombramiento y numeración de la red, el control de acceso a los servicios, el control de los patrones de tráfico a través de la definición de las métricas de las trayectorias, y la restricción de los avisos de red provocados por los protocolos de enrutamiento. Se tiene que considerar que un buen diseño de red no debe contener hosts de usuarios finales en el Backbone, esto ayudará a liberar el Backbone para que no actúe como una trayectoria de tráfico entre grupos de trabajo en diferentes edificios, o de grupos de trabajo hacia los servidores del campus.

La capa de Distribución tiene muchas funciones, incluyendo el control de acceso a los recursos por razones de seguridad y el control del tráfico de la red que atraviesa al Backbone por razones de funcionamiento. Esta capa a menudo delimita los dominios de Broadcast (aunque esto también puede hacerse en el Backbone). Si se planea implementar VLANs, la capa de Distribución puede ser configurada para encaminar el tráfico entre VLANs.

Esta capa permite que el Backbone conecte diversos sitios mientras mantiene un alto rendimiento. Para mantener un buen funcionamiento en el Backbone, la capa de Distribución puede redistribuir el ancho de banda entre los protocolos de enrutamiento de la Capa de Acceso y optimizar los protocolos de enrutamiento del Backbone. Por ejemplo, la capa de Distribución puede redistribuir entre el *Routing Table Maintenance Protocol*

(RTMP) de AppleTalk en la capa de Acceso y el *Enhance IGRP* de AppleTalk en el Backbone.

Para mejorar el funcionamiento de los protocolos de enrutamiento, la capa de Distribución puede sumarizar las rutas de la capa de Acceso. Para algunas redes, esta capa ofrece una ruta por omisión para los enrutadores de la capa de Acceso y solo trabaja con protocolos de enrutamiento dinámico cuando hay comunicación con los enrutadores del Backbone.

Otra de las funciones que desempeña esta capa es la Conversión de red. Con la conversión de direcciones, los dispositivos en la capa de Acceso pueden usar direcciones privadas. Esta función convierte las direcciones privadas en direcciones legítimas de Internet para que los paquetes puedan atravesar el resto de las redes internas de la organización o Internet.

En otras palabras, esta Capa puede desempeñar muchos roles, incluyendo la implementación de las siguientes funciones:

- Políticas,
- Seguridad,
- Agregación de direcciones,
- Acceso departamental y de grupos de trabajo,
- Definición de dominios de broadcast y multicast,
- Enrutamiento entre VLANs,
- Conversión de Medio físico,
- Redistribución entre dominios de enrutamiento,
- Demarcación entre los protocolos de enrutamiento dinámicos y estáticos.

2.1.2.3 Capa de Acceso

La Capa de Acceso provee a los usuarios acceso hacia los segmentos locales de la red. Es caracterizada por los anchos de banda compartidos y conmutados de las redes LAN en el ambiente del campus. La microsegmentación, usando switches, provee un gran ancho de banda para los grupos de trabajo gracias a la división de los dominios de colisión en los segmentos Ethernet y reduce el número de hosts capturando el token en las redes LAN de Token Ring.

2.1.2.3.1 Funciones de la Capa de Acceso

La Capa de Acceso conecta a los usuarios a las redes LAN y además conecta a las redes LAN con los Backbones del Campus. Esta aproximación permite a los diseñadores distribuir los servicios a través de los CPUs de los hosts que operan en esta capa. Esta capa permite la segmentación lógica de la red y el agrupamiento de los usuarios basándose en los intereses comunes de administración. Tradicionalmente, esta segmentación se basa en fronteras organizacionales como lo son la Mercadotecnia, Administración e Ingeniería. Sin embargo, la tecnología VLAN permite que este agrupamiento se base en la asociación o en la asignación dinámica. Desde la perspectiva de administración y control, la principal función de la Capa de Acceso es aislar el tráfico

de Broadcast para un grupo individual de trabajo o LAN. Los usuarios remotos vía dial-up también son conectados en esta capa.

Los switches son implementados en la capa de Acceso del campus de la red para dividir el ancho de banda en base a dominios después de conocer aquellas aplicaciones que requieren un gran ancho de banda y que no pueden soportar el retraso variable característico del ancho de banda compartido.

Para las corporaciones que incluyen sucursales más pequeñas y oficinas para ambientes *(SOHO: Small Office / Home Office),* la Capa de Acceso puede proporcionar el acceso a la red interna corporativa mediante el uso de tecnologías de área amplia como lo son ISND, Frame Relay, líneas telefónicas digitales o líneas análogas para módems. Las características de enrutamiento como el enrutamiento *dial-on-demand* (DDR) y el enrutamiento estático se pueden implementar para controlar la utilización del ancho de banda y reducir los costos para los enlaces remotos en la capa de Acceso. (DDR mantiene un enlace inactivo excepto cuando cierto tipo de tráfico específico necesita ser enviado).

2.2 Modelos de Redundancia

Cuando se diseña una topología de red para un cliente que tiene sistemas críticos, servicios, o enlaces de red; se debe determinar la posibilidad de falla de estos componentes e implementar redundancia donde sea necesario.

2.2.1 Redundancia en Servidores

En algunos ambientes, los servidores de archivos completamente redundantes pueden ser recomendados. Por ejemplo, en una compañía donde los trabajadores deben acceder los datos para comprar y vender existencias, los datos deben ser duplicados en dos o más servidores redundantes. Estos servidores deben estar en diferentes redes y conectados a diferentes fuentes de poder.

Si una redundancia completa de servidores no es factible debido a las consideraciones de costo, el duplicado de los discos duros de los servidores es una buena opción. En este caso existen dos opciones: la sincronización de dos discos duros bajo el mismo controlador, a esto se le llama *disk mirroring*, y la técnica llamada *disk duplexing* donde los dos discos utilizados son controlados por diferente controlador.

2.2.2 Redundancia en enrutadores

El diseño de enrutadores redundantes tiene dos propósitos: el balanceo de carga y la minimización de tiempos muertos.

Muchos de los protocolos de enrutamiento IP pueden balancear carga a través de seis enlaces paralelos de igual costo. Para soportar el balanceo de carga se debe mantener

una consistencia en el ancho de banda dentro de alguna capa del modelo jerárquico esto para que todos las rutas tengan el mismo costo.

Los protocolos de enrutamiento que se basan en saltos hacen el balanceo de carga sobre rutas con ancho de banda desigual mientras que el conteo de saltos sea igual. Una vez que el enlace más lento se satura, el enlace de mas alta capacidad no puede ser llenado, este efecto es llamado *pinhole congestion*. Este efecto puede ser evitado diseñando enlaces de igual ancho de banda dentro de alguna capa del modelo jerárquico o también usando un protocolo de enrutamiento que considere al ancho de banda dentro del conteo.

El balanceo de carga IP depende de que modo de conmutación se esta utilizando en el enrutador. El modo de conmutación *Process* hace el balanceo paquete por paquete. El proceso de conmutación *Fast* balancean carga destino a destino.

Mantener el ancho de banda consistente en alguna capa del modelo jerárquico facilita el balanceo de carga, otra razón para mantener el ancho de banda consistente dentro de alguna capa de lo modelo jerárquico se debe a que los protocolos de enrutamiento convergen mucho más rápido si existen múltiples rutas con igual costo hacia la red destino.

Además de facilitar el balanceo de carga, los enrutadores redundantes minimizan los tiempos muertos.

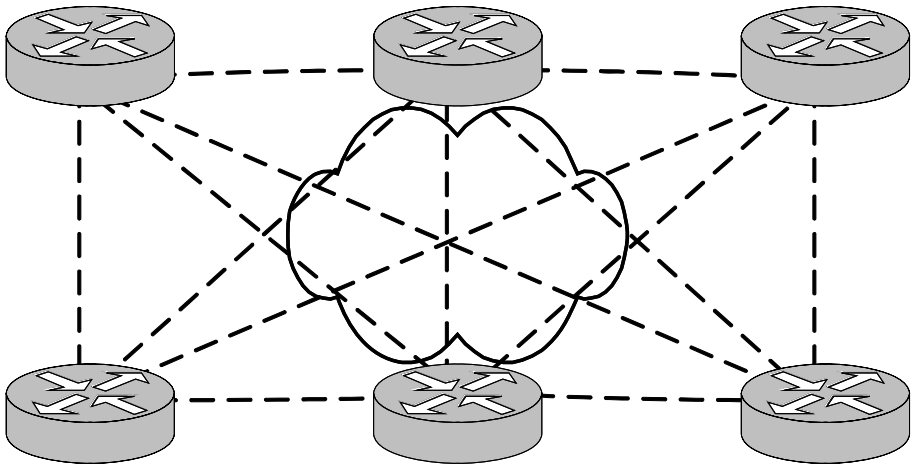
Usando redundancia, diseños de redes acopladas, se puede minimizar el efecto de las fallas en los enlaces. Dependiendo del tiempo de convergencia de los protocolos de enrutamiento usados, una simple falla en el enlace no tendrá un efecto catastrófico.

2.2.2.1 Diseño Completamente Mallado (Full Mesh)

Una red puede ser diseñada completamente mallada o parcialmente mallada. Una red completamente mallada provee redundancia completa. También provee buen funcionamiento porque existe solo un salto entre dos sitios cualesquiera.

El número de enlaces en una red completamente mallada es de $n(n-1)/2$, donde n es el número de enrutadores. Cada enrutador es conectado a todos los demás enrutadores. El resultado se divide entre 2 para evitar que se tengan dos diferentes enlaces del enrutador X al enrutador Y y del enrutador Y al enrutador X.

El diseño completamente mallado puede ser caro de implementar debido al número de enlaces requeridos. Además, existen limitaciones prácticas para escalar grupos de enrutadores que difunden actualizaciones de enrutamiento así como anuncios de servicios. Como el número de puntos de enrutamiento aumenta, la cantidad del ancho de banda y los recursos del CPU dedicados a los procesos de broadcast se incrementan. En la Figura No. 1 se muestra este diseño.



(6*5)/2= 15 circuitos

Figura No 1. Diseño Completamente Mallado

2.2.2.2 Diseño Parcialmente Mallado (Partial Mesh)

Debemos mantener el tráfico de broadcast menor al 20% del ancho de banda de cada enlace para limitar el número de puntos de enrutamiento que puedan intercambiar las tablas de enrutamiento o los anuncios de servicios. Cuando se planea la redundancia, se debe partir de lo simple: un diseño jerárquico. El diseño jerárquico y redundante clásico se muestra en la figura No. 2. Este diseño utiliza un diseño parcialmente mallado más que una arquitectura completamente mallada.

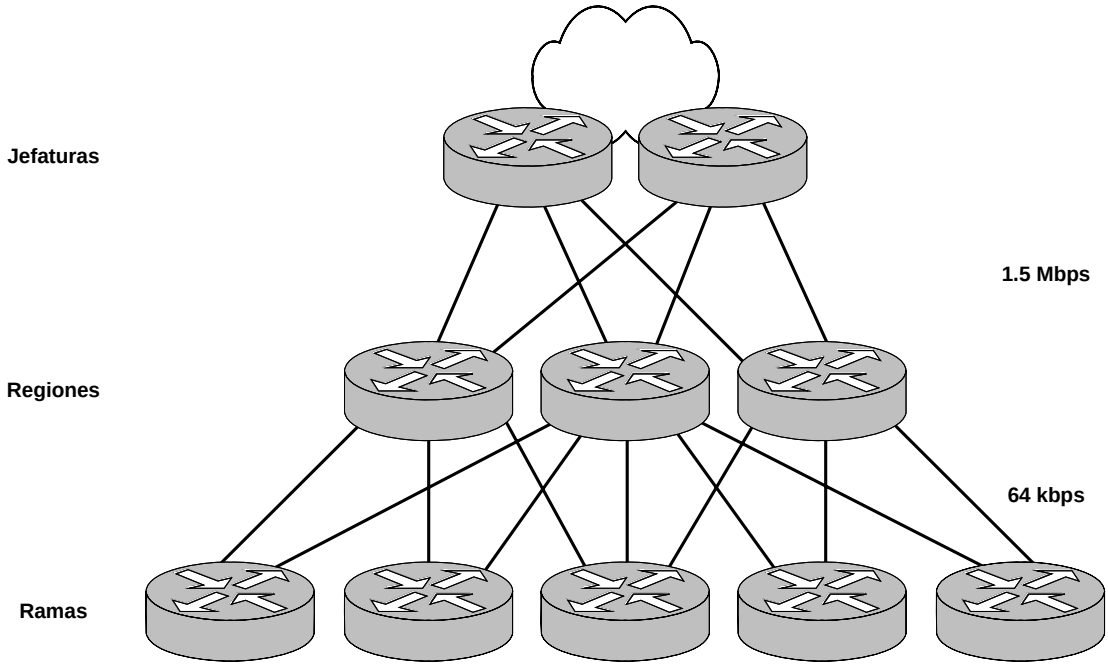


Figura No 2. Diseño Parcialmente Mallado

2.2.3 Redundancia en el Medio Físico

Cuando se utilizan aplicaciones criticas, es a menudo necesario proveer redundancia en el medio físico.

En las redes conmutadas, los switches pueden tener enlaces redundantes entre ellos. Dado que los enlaces WAN son a menudo un elemento crítico en el funcionamiento de la red, la redundancia en el medio es desplegada en los ambientes WAN. Los enlaces de respaldo pueden estar inactivos hasta que algunos de los enlaces primarios fallen o se congestione de tráfico.

A menudo los enlaces de respaldo usan tecnologías diferentes. Por ejemplo, una línea dedicada puede estar en paralelo con una línea telefónica de respaldo o con un circuito ISDN. Si se esta usando lo que se llama rutas estáticas flotantes, se puede especificar que la ruta de respaldo tiene una distancia administrativa mayor, esto no es usualmente utilizado a menos que la ruta primaria falle (se “caiga”).

Cuando se provee enlaces de respaldo, se debe aprender lo más que sea posible sobre el actual circuito de enrutamiento físico. Diferentes proveedores usan a menudo las mismas facilidades, entendiendo que su enlace de respaldo es susceptible a las mismas fallas que su enlace primario. La ruta de respaldo debe ser realmente confiable y segura.

El proceso de respaldo puede ser combinado con el balanceo de carga y la agregación de canales. Agregar canales significa que un enrutador puede mantener multiples canales B de ISDN a medida que los requerimientos de ancho de banda se incrementan. *Multilink Point-to-Point Protocol (MPPP)* es una norma de la *Internet Engineering Task Force* (IETF) para la agregación de canales B de ISDN. MPPP no especifica la manera en que el enrutador pueda lograr el proceso de decisión para activar más canales B. En vez de eso, busca asegurarse de que los paquetes lleguen con la secuencia correcta en el enrutador destino. Entonces, los datos son encapsulados con PPP y al datagrama se le da un número de secuencia. En el enrutador destino, PPP utiliza este número de secuencia para recrear el flujo original de datos. La canalización múltiple aparece como un solo enlace lógico para los protocolos de capas mayores.

2.3 Modelo Seguro

Las topologías seguras por lo general son diseñas usando *firewalls*. Un firewall protege a una red de otra red no confiable. Esta protección puede ser implementada de diferentes maneras, en inicio, un firewall es un par de mecanismos: uno se encarga de bloquear tráfico y el otro permite el flujo del mismo. Algunos firewalls hacen gran énfasis en el bloqueo del tráfico, y otros hacen énfasis en permitir el tráfico.

2.3.1 Sistema Firewall de Tres Partes

El sistema clásico de firewall, llamado Sistema Firewall de Tres Partes, tiene tres capas especiales:

- Una red LAN aislada que es un búfer entre la red interna del corporativo y el mundo exterior (La red LAN Aislada es llamada la zona desmilitarizada en alguna literatura).
- Un enrutador que actúa como un filtro interno de paquetes entre la red interna del corporativo y la red LAN Aislada.
- Otro enrutador que actúa como un filtro externo entre la red LAN Aislada y la red externa o Internet.

En la Figura No. 3 se muestra este sistema.

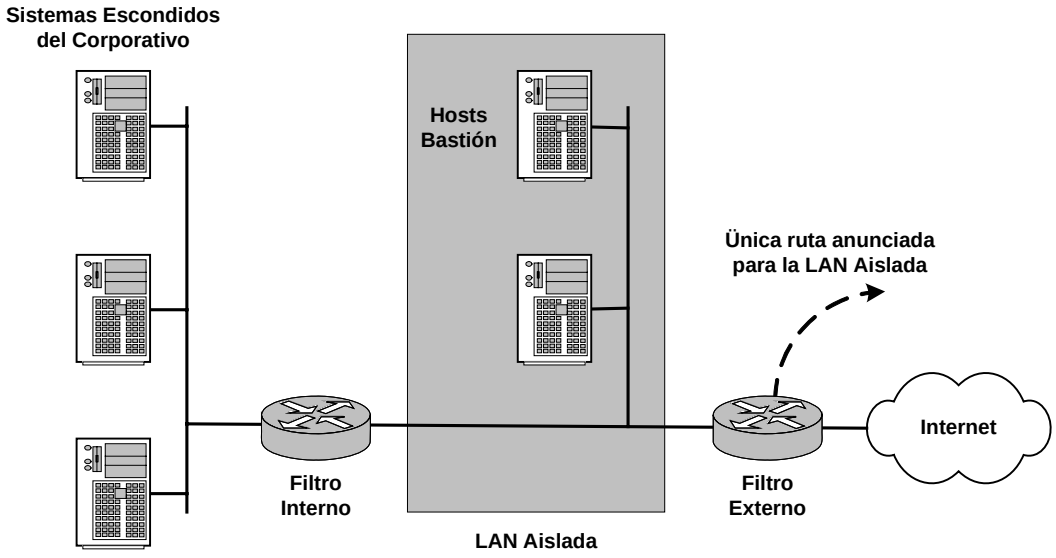


Figura No 3. Sistema Firewall de tres Partes

Los servicios disponibles para los usuarios remotos están alojados en los hosts de la red LAN Aislada, algunos de los servicios disponibles son los siguientes:

- Servidor de FTP Anónimo,
- Servidor Web,
- Domain Name Service (DNS),
- Telnet, y
- Software especializado para seguridad como el TACACS+ (Terminal Access Control Access Control System +).

La red LAN Aislada tiene una única dirección de red que es diferente a la dirección de la red LAN. La red LAN Aislada es la única visible para el mundo exterior. En el filtro externo podemos anunciar solo la ruta de la red LAN Aislada.

Si un usuario interno necesita tener acceso a los servicios de Internet, se debe permitir que el tráfico TCP de salida fluya desde la red LAN interna. Y solo se permitirá que regresen los paquetes TCP con ACK o bits RST. La palabra clave establecida es usada para indicar paquetes que contengan el ACK o bits RST. Todos lo demás paquetes TCP deben ser bloqueados debido a que el nuevo tráfico de entrada TCP podría ser resultado de sesiones de *Hackers* que intentan establecer conexión con los hosts internos. La siguiente lista resume algunas reglas para el Sistema Firewall de tres partes:

- El enrutador interno utilizado para el filtrado de paquetes debe permitir la entrada de tráfico TCP externo que provenga de sesiones ya establecidas.
- El enrutador externo utilizado para el filtrado de paquetes debe permitir la entrada de tráfico TCP externo que provenga de sesiones TCP ya establecidas.
- El enrutador externo utilizado para el filtrado de paquetes debe permitir también el flujo de tráfico hacia puertos específicos TCP o UDP configurados en los hosts de la red LAN Aislada (esto incluye paquetes de sincronización TCP que son usados para establecer las sesiones).

Los enrutadores utilizados como firewalls y los hosts son puntos de entrada para los Hackers, por eso debemos bloquear el tráfico de extraña procedencia en ellos.

Se debe mantener los hosts de la red LAN Interna y los enrutadores utilizados como firewalls ejecutando la mínima cantidad de programas, estos programas deben ser lo más sencillo posible, ya que los programas sencillos tiene menos *bugs* (o errores de programación) que los programas complejos. Los bugs introducen posibilidad de entrada para los Hackers.

Además de lo anterior, no se deben habilitar servicios o conexiones innecesarias en el enrutador externo que trabaja como filtro. A continuación se muestra una lista de implementación de sugerencias para el filtro externo:

1. Deshabilitar el acceso remoto por medio de Telnet (terminales virtuales no definidas),
2. Usar solo enrutamiento estático,
3. No habilitarlo como un servidor de TFTP,
4. Usar encriptación de passwords,
5. Deshabilitar el servicio de proxy ARP,
6. Deshabilitar el servicio *finger*,
7. Deshabilitar redireccionamiento IP,
8. Deshabilitar el almacenamiento de rutas IP y,
9. No habilitarlo como un servidor MacIP.

3. Modelos de Diseño del Campus

El diseño típico en un edificio, como el que se muestra en la figura 1, será usado en los ejemplos que siguen. Estos ejemplos asumen que los hosts deben acceder a servidores y a otros hosts. Los servidores pueden identificarse como aquéllos que son locales para un grupo de trabajo o para un piso del edificio, y aquéllos usados más extensamente (edificios, campus, o empresas). Se requerirán conexiones para hosts en un grupo de trabajo, el cual está separado para cada piso del edificio. Un closet de comunicaciones esta disponible en cada piso del edificio para conectar los hosts y los servidores locales de cada piso del edificio. La vertical que comunica a todos los pisos del edificio y provee una ruta de cableado para interconectar los grupos de trabajo localizados a lo largo de los edificios. En el sótano del edificio se aloja un Centro de Cómputo donde los servidores que tienen más trabajo se localizan, junto con las conexiones requeridas para otros edificios y sitios.

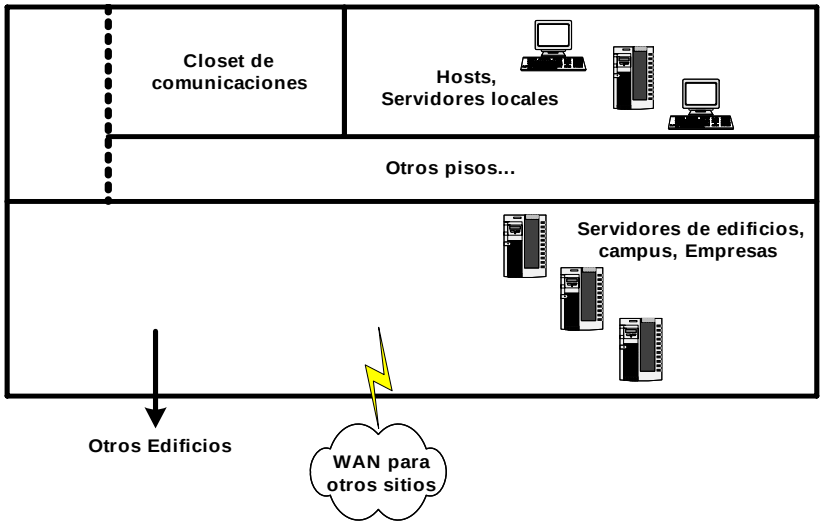


Figura 1. Diseño del Edificio.

En general las recomendaciones de cableado, requieren fibra entre las verticales y los pisos, y en la canalización que típicamente conectan los edificios al campus. La fibra permite utilizar un ancho de banda como sea necesario (100BaseFX, 1000BaseX, 10G) mientras provee un enlace confiable que es resistente a las fuentes de interferencia magnética (EMI). Los componentes activos de red (bridges, switches, enrutadores) están típicamente localizados en los closets de comunicaciones en cada piso, y en el Centro de Cómputo, localizado en el sótano. El cable UTP categoría 5, 5e ó 6, en muchos casos, debe ser usado para enlazar hosts y servidores locales con los componentes activos en los closets de comunicaciones. Un cable UTP categoría 5 ó 5e es generalmente considerado para ser usado a velocidades de hasta 100 Mbps, sobre una distancia máxima de 100 metros.

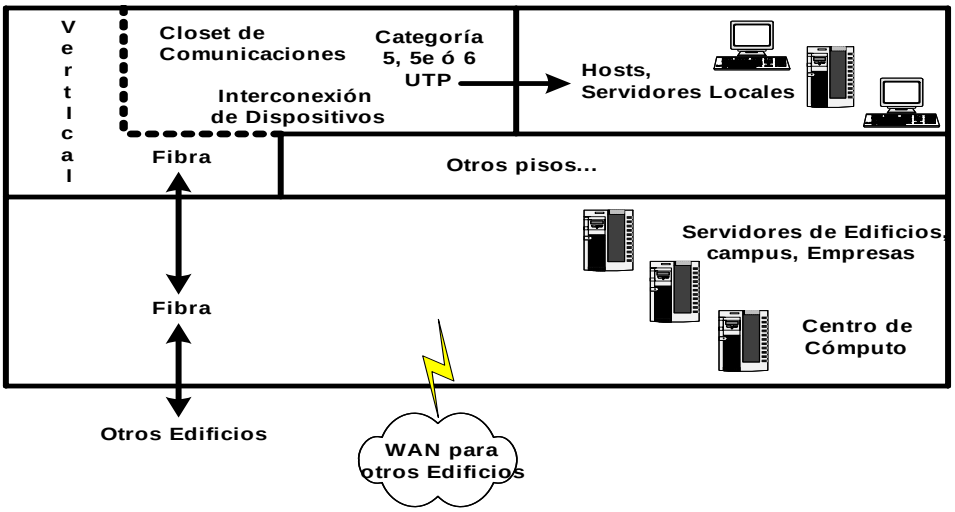


Figura 2. Cableado.

3.1 Backbones Distribuidos

3.1.1 Backbones Distribuidos en un Edificio

En el modelo de Backbone Distribuido, los enrutadores conectan cada piso al Backbone por medio de la vertical. Actualmente el Backbone se sustituye por un switch Fast Ethernet (Figura 3). Este diseño tiene el beneficio de distribuir las conexiones por el Backbone y por ello se elimina cualquier punto de falla.

Este diseño tiene desventajas. Por ejemplo: la existencia de múltiples redes IP dentro de un edificio, reduce la facilidad de agregar usuarios o moverlos, y cambios que pueden ser realizados en la estructura de la organización. Además, este diseño tiende a ser más caro por los enrutadores utilizados.

Nótese que en este diseño, los hosts no están conectados al Backbone. Este es un criterio importante en el plan de diseño, que debe seguirse para el diseño. El Backbone solamente debe ser usado como una ruta para transitar entre redes locales, y no como una red local. Este criterio mantiene el Backbone más estable, con facilidad para administrar el tráfico y la capacidad de planificación, refuerza sobretodo, la escalabilidad para un rediseño futuro. Las posibles excepciones incluyen servidores de trabajo pesado (como servidores que proveen DNS o SMTP). Esto porque, los servicios de gran carga no deben de estar separados de la capa de acceso, y más aún si son de uso local.

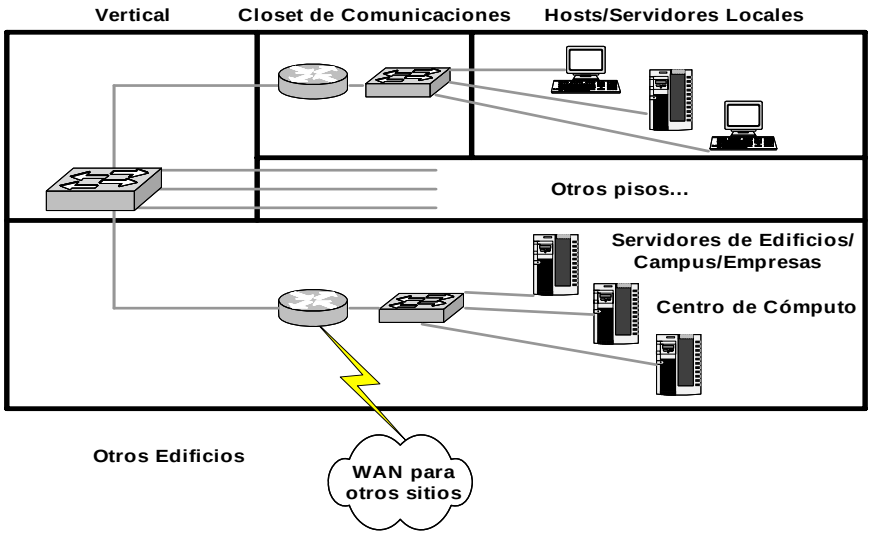


Figura 3. Modelo de Backbone Distribuido en un Edificio usando switch.

3.1.2 Backbones Distribuidos entre Edificios

El Backbone Distribuido en el campus es una solución de recursos más eficiente que el Backbone Distribuido en un edificio. Esta solución envuelve un solo enrutador por cada edificio, típicamente localizado en el Centro de Cómputo, con switches proveyendo acceso a los usuarios a lo largo del edificio, la conexión entre edificios actualmente es desplegada con switch Fast Ethernet (Figura 4). Con menos redes lógicas por edificio, con la facilidad de agregar usuarios o moverlos, y con la posibilidad de realizar cambios de acuerdo a la estructura de la organización. Este modelo tiene una sola desventaja, es la falta de flexibilidad en conexiones con otros edificios del campus. El switcheo podría ser fácilmente desplegado en el edificio y también en el campus.

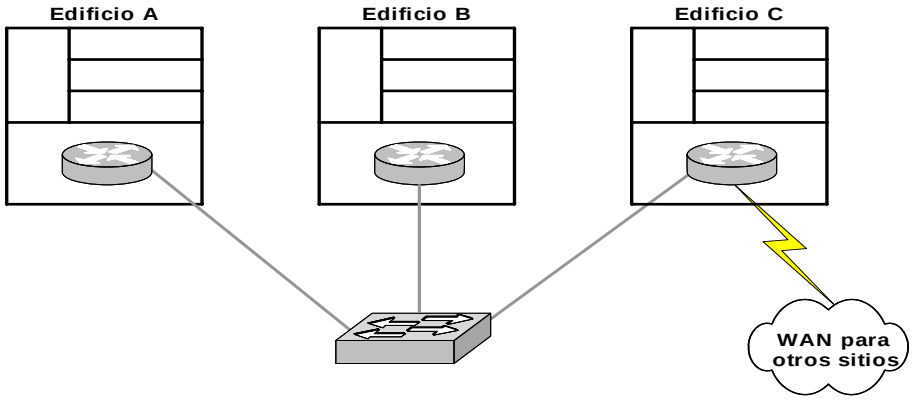


Figura 4. Modelo de Backbone Distribuido entre Edificios usando Switch.

3.2 Backbones Colapsados

3.2.1 Backbones Colapsados dentro de un Edificio usando Enrutadores y Switches

Generalmente el Backbone Colapsado representa mucho más flexibilidad y rentabilidad para cablear un edificio. En este caso, el Backbone es "colapsado" dentro de un solo switch o enrutador, haciendo que el *backplane* del switch actúe como el Backbone de la red. Los switches en cada piso son utilizados para conectar los hosts en el grupo de trabajo, y cada uno comunica una interfaz LAN con el enrutador. Este modelo podría hacer el movimiento de usuarios un poco más fácil que en el modelo de Backbone distribuido, pero la solución no es todavía ideal. Ya que el enrutador representa un solo punto de falla, esta situación podría ser corregida por el uso de un segundo enrutador conectado con el switch.

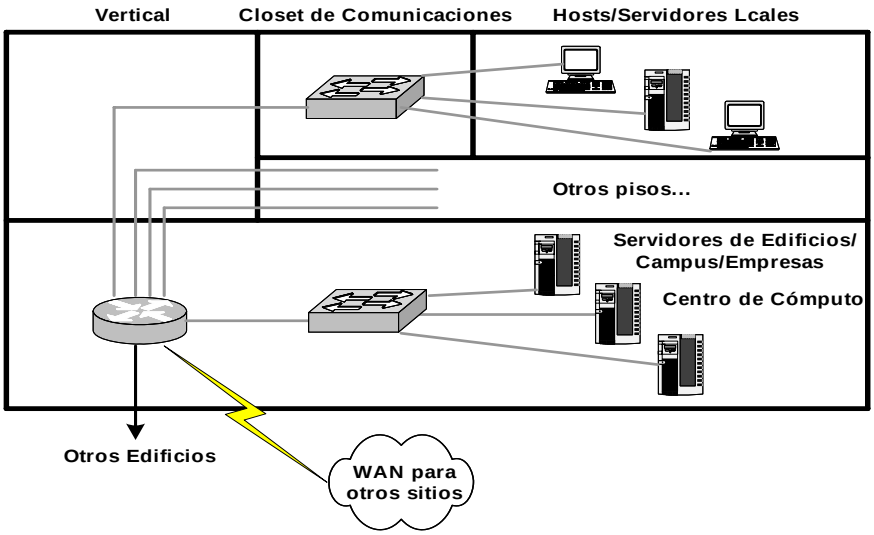


Figura 5. Modelo de Backbone Colapsado dentro de un Edificio usando enrutadores y switches.

3.3 Modelo con VLANs

3.3.1 Modelo de Backbone Colapsado dentro de un Edificio usando VLANs.

El diseño del Backbone colapsado puede fácilmente, ser extendido para el uso de VLANs, simplemente agregando otro switch Fast Ethernet en el Centro de Cómputo. El *backplane* del switch ahora se convierte en el Backbone colapsado para el edificio. En este caso, el enrutador tiene un puerto Ethernet separado para cada VLAN o puede utilizarse una sola interfaz física con varias interfaces virtuales configuradas, incluso el switch que se encuentra antes del enrutador puede hacer el enrutamiento entre VLANs con la condición que el switch soporte capa 3. El enrutador también provee los puntos de conexión final

para acceder otras redes de edificios, como antes visto en el modelo de Backbone colapsado usando enrutadores y switches.

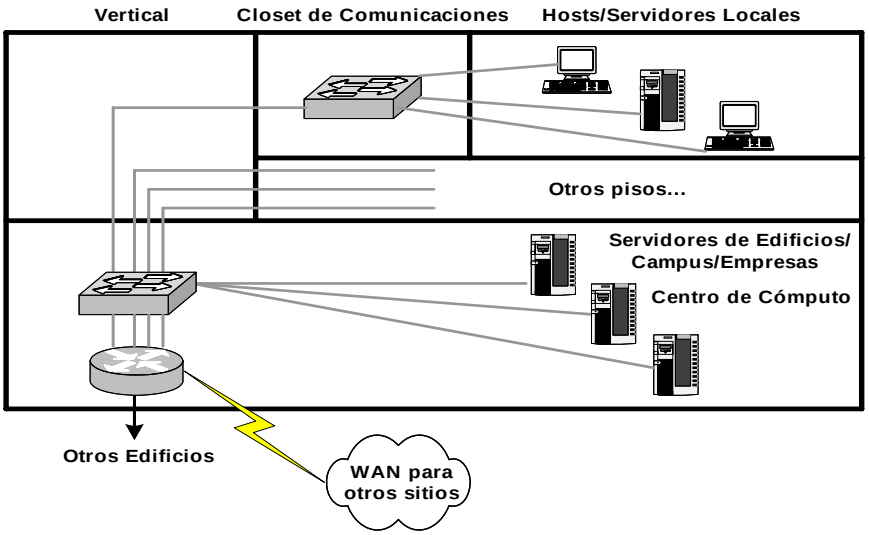


Figura 6. Modelo de Backbone Colapsado dentro de un Edificio usando VLANs.

3.3.2 Modelo de Backbone Colapsado dentro de un Edificio usando VLANs con servidores centralizados.

El uso de VLANs provee más flexibilidad en la ubicación física de hosts y de servidores. Los hosts pueden ubicarse físicamente en cualquier parte del edificio y aún pueden permanecer en la misma LAN. Además, un usuario puede permanecer físicamente en su lugar actual y moverlo a una nueva asignación lógica LAN (VLAN). Todos los servidores en el edificio pueden ubicarse físicamente en un mismo lugar (Granja de Servidores), y permanecer lógicamente en LANs separadas.

La troncal de enlaces entre pisos debe ser Fast Ethernet o Gigabit Ethernet, y todas las tramas podrían portar el VLAN ID. La conexión del enrutador al Backbone del switch puede ser Fast Ethernet y recibir el VLAN ID. Se puede configurar interfaces separadas, por cada VLAN o configurarse una sola interfaz física en varias lógicas, y el enrutador o el switch capa 3 del Centro de Cómputo dirigiría el enrutamiento entre VLANs.

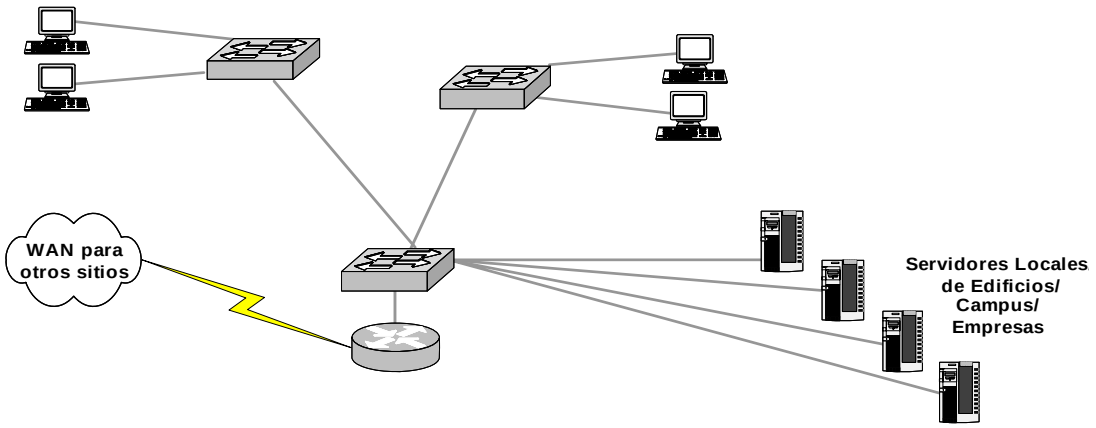


Figura 7. Modelo de Backbone Colapsado dentro de un Edificio usando VLANs con servidores centralizados.

3.3.3 Modelo de Backbone Colapsado dentro del Campus usando VLANs.

El concepto de Backbone colapsado podría ser tomado más allá para incluir el campus entero. Un switch podría actuar como Backbone para el campus completo, el cual podría permitir máxima flexibilidad en el movimiento de usuarios alrededor del campus, físicamente o lógicamente. Todos los servidores pueden ubicarse físicamente en el mismo lugar para una administración más fácil.

Por supuesto, esta configuración crea un espacio en el direccionamiento que puede limitar la escalabilidad como el crecimiento de la empresa, que puede ser solucionado utilizando *NAT*. El crecimiento potencial, debe considerarse como una variable importante en cualquier diseño de red.

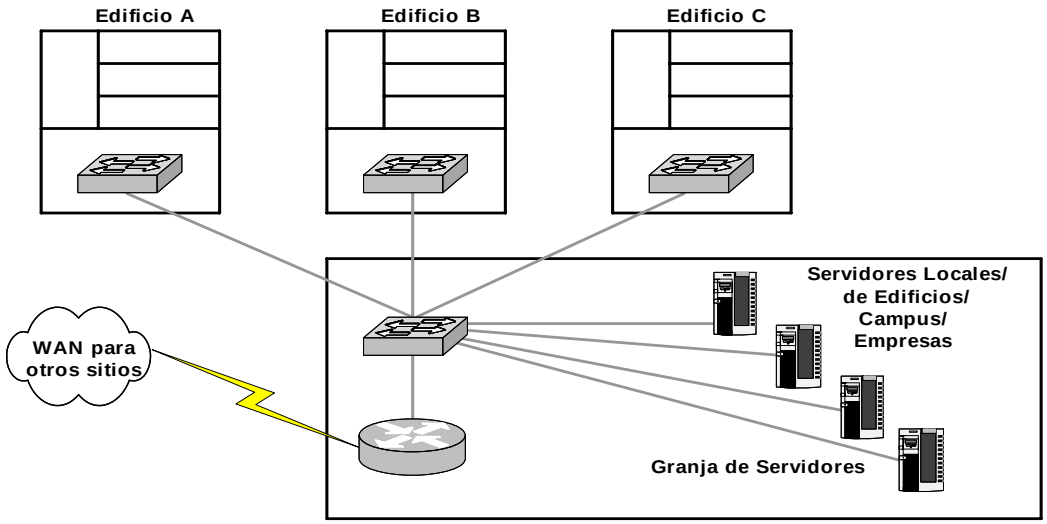


Figura 6. Modelo de Backbone Colapsado dentro de un Campus usando VLANs.

3.3.4 Ventajas del Modelo con VLANs

Modelo de Backbone Colapsado dentro de un Edificio usando VLANs.

- Se puede utilizar el modelo de Backbone colapsado para el uso de VLANs, simplemente agregando otro switch Ethernet en el Centro de Cómputo.
- El enrutamiento lo realiza el enrutador o switch capa 3 localizados en el Centro de Cómputo.
- El *backplane* del switch se convierte en el Backbone de la red por lo que es de gran capacidad de transferencia.

Modelo de Backbone Colapsado dentro de un Edificio usando VLANs con servidores centralizados.

- Flexibilidad en la ubicación física de los hosts y servidores.
- Separación lógica de equipos de acuerdo al grupo de trabajo sin necesidad de moverlos físicamente.
- A parte de la seguridad en administración de los servidores se logra seguridad física, ya que todos se localizan en una Granja de Servidores en el Centro de Cómputo.

Modelo de Backbone Colapsado dentro de un campus usando VLANs.

- El switch del Centro de Cómputo podría actuar como Backbone para el campus completo.
- Flexibilidad en el movimiento de usuarios alrededor del campus, físicamente o lógicamente.
- Todos los servidores podrían se posicionados en un solo lugar para una administración más fácil.

3.3.5 Desventajas del Modelo con VLANs

Modelo de Backbone Colapsado dentro de un Edificio usando VLANs.

- El enrutador es un punto de falla para la conexión entre otros edificios, incluso en el enrutamiento si lo realiza este.
- Los switches de alta densidad de puertos son muy caros.

Modelo de Backbone Colapsado dentro de un Edificio usando VLANs con servidores centralizados.

- El enrutador es un punto de falla para la conexión entre otros edificios.
- Los switches de alta densidad de puertos son muy caros.

Modelo de Backbone Colapsado dentro de un campus usando VLANs.

- Esta configuración crea un espacio en el direccionamiento que puede limitar la escalabilidad como el crecimiento de la red.
- El enrutador es un punto de falla para la conexión entre otros edificios fuera del campus.
- Los switches de alta densidad de puertos son muy caros.

3.4 Modelo Multicapas basado en Hardware

El Modelo Multicapas basado en Hardware provee escalabilidad y estabilidad a diferencia del Modelo de Backbone Colapsado dentro de un edificio usando enrutadores y switches, mientras que también tiene el desempeño del Modelo de Backbone Colapsado dentro de un edificio usando VLANs. Este modelo toma ventaja del enrutamiento basado en hardware, switcheo en capa 3 y coloca el enrutamiento en el lugar que le corresponde tomando como referencia el modelo de tres capas (capa de Acceso, capa de Distribución y el Backbone). Sin embargo, no ignora el switcheo en capa 2. De hecho, busca romper el equilibrio óptimo del switcheo en capa 3 que se usa para el control, considerando que el switcheo de capa 2 se usa para el *forwarding* de datos eficiente. La figura 7 ilustra un ejemplo de red usando el Modelo Multicapa.

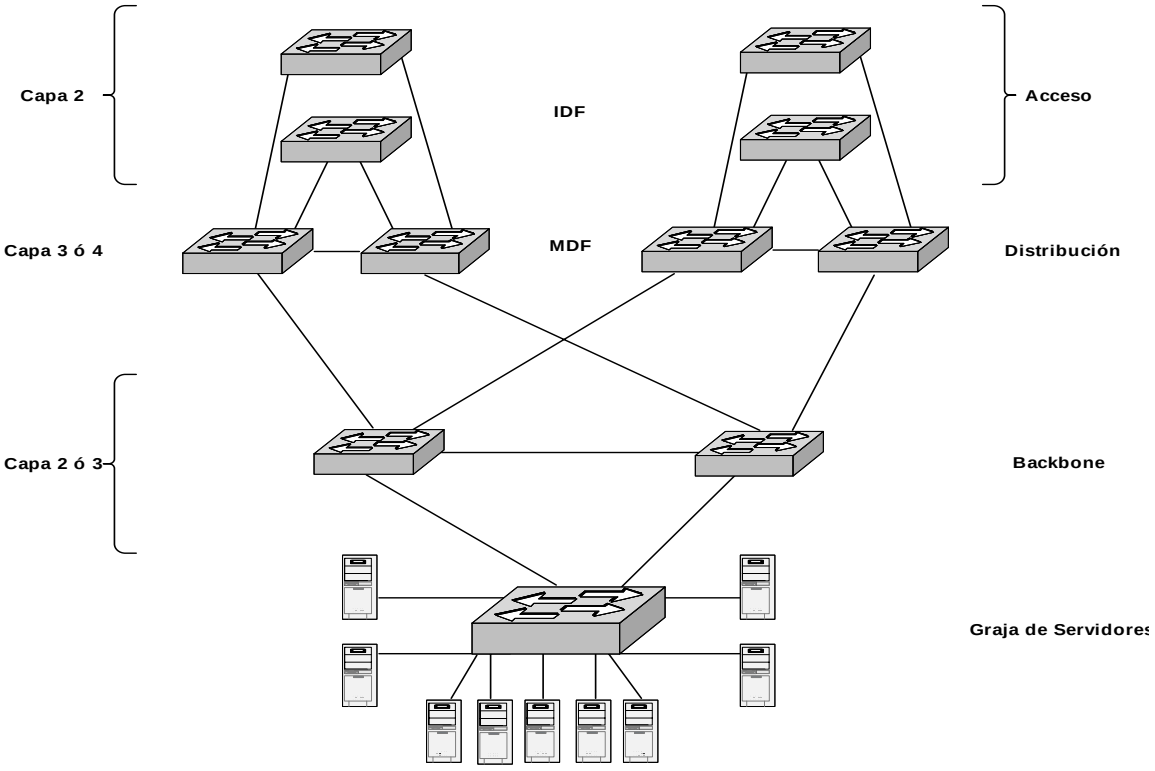


Figura 7. Modelo Multicapa.

Cada IDF/MDF se agrupa en módulos en el diseño. La figura anterior muestra dos módulos. Los switches del IDF de la capa de acceso usan el *forwarding* para proveer las cantidades de ancho de banda efectivo. Los switches del MDF de la capa de distribución proveen el control de la capa 3 que es requerida en todas las redes grandes. Esos módulos IDF/MDF entonces se conectan a través de una variedad de Backbones de capa 2 ó capa 3.

En general, el Modelo Multicapa es el más recomendado para diseño de campus de empresas por muchas razones:

Primero, el uso de enrutadores provee un adecuado control en capa 3. Permite tener todos lo beneficios que tiene el enrutamiento. Un diseño multicapa es escalable y flexible, tiene alto desempeño, y fácil para administrar.

Segundo, como su nombre lo dice, el Modelo Muticapa ofrece jerarquía. En redes jerárquicas, se definen capas con papeles específicos para permitir consistentes y grandes diseños. Esto le permite a cada capa del modelo de tres capas reunir requisitos únicos y específicos de diseño.

Tercero, este modelo es muy modular. Hay muchos beneficios de un diseño modular, incluyendo los siguientes:

- Es fácil crecer la red.
- El ancho de banda crece como módulos adicionales que son agregados.
- Las redes modulares son fáciles de entender, de solucionar problemas, y de mantener.
- La red puede usar configuraciones *cookie cutter*. Esta consiste en ahorrar dolores de cabeza a los administradores de la red, mientras también reduce la vulnerabilidad de errores de la configuración.
- Es más fácil migrar a una red modular. La red vieja puede aparecer como otro módulo (aunque no tiene el diseño consistente y configuraciones de módulos en la nueva red).
- Las redes modulares permiten patrones de tráfico consistentes y determinísticos.
- El diseño modular promueve el balanceo de carga y redundancia.
- Es mucho más fácil proporcionar un *failover* rápido en un diseño consistente, el diseño modular es utilizado en los diseños menos estructurados. Se define bien la topología en ambas capas, capa 2 y capa 3, y tiene el beneficio de la convergencia.
- Las redes modulares permiten sustituir fácilmente las tecnologías entre redes. No sólo permite más libertad a las organizaciones en el diseño inicial (por ejemplo, el Backbone puede ser Ethernet o ATM), esto hace más fácil la actualización de la red.

4. Guía de Diseño de Red

4.1 Caracterización de la red existente.

4.1.1 Objetivos

- Identificar todos los datos que deben de reunir para caracterizar una red existente.
- Documentar las aplicaciones, protocolos, topología y número de usuarios.
- Documentar los negocios en cuestión que son relevantes para el proyecto de diseño de red.
- Evaluar la salud de la red existente y realizar las conclusiones acerca del futuro crecimiento.

4.1.2 Caracterizando la Red

Para caracterizar la red es necesario identificar cualquier cuello de botella, determinar si el anticipado crecimiento de la red causará algún problema, reconocer sistemas legados que deben ser incorporados en el nuevo diseño y reconocer negocios en cuestión que son relevantes para el proyecto de diseño de red (los negocios en cuestión son negocios relacionados con el diseño de la red que pueden ser una limitación).

4.1.2.1 Obtención de Datos Administrativos

Los datos administrativos ayudan a determinar los objetivos de los negocios de la compañía, estructura corporativa, estructura geográfica, personal actual y futuro, y las políticas que pueden afectar el diseño de la red:

- *Objetivos de los negocios:* Determinar los objetivos de los negocios mayores de la compañía para el siguiente año, y los siguientes cinco años. Esta información es importante para diseñar una red que provea la escalabilidad requerida. Investigar la industria del cliente y la competencia. Con el conocimiento de los negocios del cliente es posible proporcionar una mejor solución para las necesidades que requiere el usuario.
- *Estructura corporativa:* El diseño final de la red usualmente refleja la estructura corporativa, así que es muy importante ser proactivos para ayudar a entender la estructura corporativa.
- *Estructura geográfica:* Hay que localizar las comunidades mayores del usuario.
- *Personal actual y futuro:* Realizar las siguientes preguntas:

    - ¿Cuánta especialización interna de la red hay?
    - ¿La compañía planea extender al personal como es requerido para apoyar el nuevo diseño de red?
    - ¿Quién ayudará a diseñar le red?
    - ¿El nuevo diseño causará cambios en las funciones de trabajo o posiblemente eliminará trabajos?

- *Políticas:* Sucesos pasados o fallas pueden ayudar a determinar áreas de problemas para el diseño de red. Formular las siguientes preguntas ayuda a identificar estos sucesos:

    - ¿Un nuevo diseño ha sido probado antes y ha fallado? ¿A quién le pertenece el diseño?
    - ¿Hay gente en el proyecto que no quiere realizar cambios?

4.1.2.2 Obtención de Datos Técnicos

Los datos técnicos ayudarán a entender las aplicaciones actuales y las planeadas a futuro, así como protocolos actuales, interconexión de dispositivos y como impactan los cuellos de botella en el desempeño de la red.

- *Aplicaciones:* Identificar las aplicaciones actuales y planes para aplicaciones futuras.
- *Flujos de Información:* Se debe analizar donde fluye la información de la organización. Si cualquier proceso de reingeniería se ha realizado recientemente, los flujos de información ya pueden documentarse. Si no, pudiera tomar tiempo considerable para hacer el análisis.
- *Datos Compartidos:* Hay que determinar donde residen los datos compartidos y quién los usa.
- *Tráfico de la Red y Acceso:* Determinar cuanto tráfico fluye de un segmento de red a otro. Determinar si datos fuera de la organización, como el Internet, son consultados.
- *Las Características de Desempeño de la Red:* Es importante entender el desempeño de las características de la red. Documentar cualquier problema, especialmente si estos continuaran existiendo aún después de que el nuevo diseño sea implantado.

Has un análisis “Baseline” del desempeño de la interconexión existente. Si la interconexión es muy grande para realizar el baseline, se deberá analizar los backbones y segmentos críticos de la red.

4.1.2.3 Herramientas para Caracterizar una Red

Si la persona que realiza esta caracterización no está familiarizada con herramientas para caracterizar la red, es recomendable buscar los sitios Web de los fabricantes para obtener más información. En seguida se describen solo algunas de las muchas herramientas disponibles que son útiles para realizar la caracterización de la red:

- Estadísticas de las interfaces
- Tamaño de la tabla de enrutamiento
- Contabilidad de paquetes IP/IPX
- RMON
- SNMP
- Analizadores de Protocolos
- Sniffers

Los analizadores de protocolos capturan y analizan el tráfico en la red, proveen estadísticas y análisis de protocolos. Algunos analizadores, incluyen inteligencia artificial para simplificar y reforzar la administración del desempeño de la red.

4.1.3 Caracterizando una Red

Esta sección provee una metodología estructurada que debe seguirse para caracterizar la red. Los procedimientos, tablas, y checklist ayudan a determinar las necesidades de la interconexión para diseñar una solución escalable.

El siguiente paso del diseño para investigar el estado de la red, es obtener una caracterización de la red que se puede obtener con los siguientes pasos:

4.1.3.1 Paso 1: *Caracterizando las Aplicaciones.*

La siguiente tabla es útil para caracterizar las aplicaciones. Las instrucciones para usar la tabla, son como sigue:

- En el campo “Nombre de la Aplicación” se debe ingresar el nombre de cada aplicación que es ejecutada en la red.
- En el campo “Tipo de Aplicación” se debe ingresar la información que ayudará a caracterizar la aplicación, por ejemplo: bases de datos, multimedia, correo electrónico, streaming, VoIP, videoconferencia, e-learning, aplicaciones on-demand, sistemas de manufactura, y así sucesivamente.
- En el campo “Número de Usuarios”, se debe ingresar el número de usuarios que accesan a cada aplicación.
- En el campo “Número de Hosts o Servidores”, se debe ingresar el número de hosts o servidores que provee cada aplicación.
- En el campo “Comentarios”, se debe agregar cualquier comentario relevante para el diseño de la red. Por ejemplo, agregar cualquier escalabilidad involucrada. Incluir cualquier información que tenga acerca de las direcciones corporativas, como planes para migrar a una aplicación.

	Nombre de Aplicación	Tipo de Aplicación	Número de Usuarios	Número de Hosts o Servidores	Comentarios
1					
2					
3					
4					
5					

Tabla 1. Resumen de Aplicaciones.

4.1.3.2 Paso 2: *Caracterizando los Protocolos.*

La siguiente tabla permite caracterizar los protocolos de la red. Las instrucciones para usar la tabla, son como sigue:

- En el campo “Nombre de Protocolo”, se debe ingresar el nombre de cada protocolo en la red.
- En el campo “Tipo de Protocolo”, se debe ingresar algún texto que facilite a identificar el protocolo, por ejemplo, protocolo capa-sesión, cliente/servidor y así sucesivamente.
- En el campo “Nombre de Usuario”, se debe ingresar el número de usuarios que utiliza cada protocolo.
- En el campo “Número de Hosts o Servidores”, se debe ingresar el número de servidores que usa cada protocolo.
- En el campo “Comentarios”, se debe ingresar cualquier comentario relevante para el diseño de la red. Por ejemplo, agregar cualquier escalabilidad involucrada. Incluir cualquier información acerca de las direcciones corporativas, como planes para migrar a un protocolo.

	Nombre de Protocolo	Tipo de Protocolo	Número de Usuarios	Número de Hosts o Servidores	Comentarios
1					
2					
3					
4					
5					

Tabla 2. Resumen de Protocolos.

4.1.3.3 Paso 3: *Documentando la Red Actual.*

Dispositivos y Topología de Red. Realice el diagrama de la topología de red (u obtener un dibujo de la red actual proporcionado por el administrador de red). Se debe incluir el tipo y velocidad de cada segmento o enlace. También hay que incluir los nombres y direcciones de la interconexión de dispositivos y servidores.

Esquema de Direccionamiento. Documente el esquema de direccionamiento usado en el diseño de red actual. El direccionamiento actual puede impactar para modificar la estructura de la red. Por ejemplo, la máscara de una subred IP actual puede limitar el número de hosts en un LAN o en una VLAN.

Relaciones Acerca de la Red. Documente cualquier relación que haya acerca de la topología actual y cualquier información adicional acerca de la arquitectura de la

interconexión que no pueda ser obvia por el diagrama de la topología. Es importante caracterizar la arquitectura de red en conjunto para ayudar a entender los patrones de flujo de datos.

4.1.3.4 Paso 4: *Identifique los Cuellos de Botella Potenciales.*

Uso de un Analizador de Protocolos para Determinar el Tráfico Local. Para identificar los cuellos de botella potenciales, se debe utilizar un analizador de protocolos y determina cuánto tráfico de la red en cada segmento no es local. Especifique cuánto tráfico atraviesa a diferentes segmentos de red, cuánto tráfico llega de otros segmentos de redes y cuánto es el tráfico que pasa a través de un segmento de red.

Caracterizando el Tráfico que no es Local. Utilice la tabla 3 para caracterizar cuánto tráfico en cada segmento de red no es Local. El uso de la tabla 3, se describe a continuación:

- En el campo “Origen y Destino son Locales”, ingrese el porcentaje de tráfico en el segmento que estés analizando.
- En el campo “Origen Local y Destino no Local”, ingrese el porcentaje de tráfico en el segmento que estés analizando.
- En el campo “Origen no Local y Destino Local”, ingrese el porcentaje de tráfico en el segmento que estés analizando.
- En el campo “Origen y Destino no Locales”, ingrese el porcentaje de tráfico en el segmento que estés analizando.

	Origen y Destino son Locales	Origen Local y Destino no Local	Origen no Local y Destino Local	Origen y Destino no Locales
Segmento 1				
Segmento 2				
Segmento 3				
Segmento 4				
Segmento 5				

Tabla 3. Caracterización de Tráfico.

4.1.3.5 Paso 5: *Identifica las Limitantes del Negocio y Entradas en el Diseño de la Red.*

Checklist de las Limitantes del Negocio. Después de hablar con el administrador, hay que verificar que tantos de los elementos de la lista ya has identificado.

- Se ha entendido la estructura corporativa.
- Se ha analizado el flujo de la información de la empresa.
- El administrador, tiene identificado operaciones o datos de misión crítica.
- El administrador, ha explicado cualquier política con respecto a protocolos o plataformas.
- El administrador, ha explicado cualquier política con respecto a soluciones abiertas versus propietarias.
- El administrador, ha explicado cualquier política con respecto a la autoridad de distribución para el diseño e implantación de la red.
- Existe una buena comprensión de la especialización técnica de los usuarios.
- Se ha investigado la industria del cliente y la competencia.
- El administrador, ha explicado cualquier política con respecto.
- Existe una conciencia de cualquier política que pueda afectar el desempeño de la red.

En general, documente cualquier cosa concerniente a las limitantes de negocio del cliente.

4.1.3.6 Paso 6: *Caracteriza la Disponibilidad de la Red Existente.*

Obtenga estadísticas del tiempo que la red queda fuera de servicio y las fallas que se presenten en los diferentes segmentos que existan en la red. Si algunos segmentos son más vulnerables a fallar, documente esos segmentos por separado. Intente obtener de los usuarios, para expresar, el costo del tiempo que la red está fuera de servicio obteniendo la información con las siguientes preguntas:

- ¿Cuál es el costo por hora que genera por departamento que la red quede fuera de servicio?
- ¿Cuál es el costo por hora que genera para la empresa que la red quede fuera de servicio?

Utilice la siguiente tabla para determinar las fallas de transmisión para cada segmento de red y de interconexión. Las siguientes instrucciones indican el uso de la tabla 4:

- En el campo “Falla de Transmisión”, ingrese el número de fallas para cada segmento en los últimos 30 años.
- En el campo “Tiempo de la Última Caída de Red”, ingrese la fecha en la cuál los usuarios experimentaron la última caída del servicio de red.
- En el campo “Duración de la Última Caída de Red”, ingrese cuanto tiempo duró la última caída.

- En el campo “Causa de la Última Caída de Red”, ingrese la causa (si se conoce) de la última caída en cada segmento.

	Falla de transmisión	Tiempo de la última caída de red	Duración de la última caída de red	Causa de la última caída de red
Segmento 1				
Segmento 2				
Segmento 3				
Segmento 4				
Segmento 5				

Tabla 4. Caracterización de Tráfico.

4.1.3.7 Paso 7: *Caracterizando el Desempeño de la Red.*

En la siguiente tabla, documente los resultados de cualquier medida de tiempo/desempeño de respuesta que hayas completado para cada host en la red:

	Host A	Host B	Host C	Host D
Host A				
Host B				
Host C				
Host D				

Tabla 5. Medida de Tiempo/Desempeño de Respuesta.

4.1.3.8 Paso 8: *Caracterizando la Confiabilidad de la Red Existente.*

Obtenga las estadísticas acerca de los segmentos mayores de red usando alguna herramienta de monitoreo como un analizador de protocolos, alguna herramienta de monitoreo de red o alguna herramienta de administración de red. Si es posible, monitoree cada segmento de red, por al menos un día. Al final del día, registre lo que el monitoreo ha visto en cada segmento de red:

- Total de Megabytes (MB)
- Total del número tramas

- Total del número de errores CRC
- Total del número de errores de la subcapa MAC (colisiones)
- Total del número de tramas de broadcast/multicast

Caracterice la confiabilidad de la red actual completando la tabla 6. Para calcular el promedio de la utilización de la red, agregue cada promedio de cada hora y divida por el número de promedios de cada hora. Para los picos de la utilización de la red, registre el promedio de cada hora más alto. (Si tiene los datos más granulares que de cada hora, registre cualquier pico a corto plazo). Para el promedio del tamaño de trama, divida el número total de MB transferidos en la red por el total del número de tramas.

Para calcular la tasa de errores del CRC, divida el número total de CRCs entre la cantidad total de Megabytes. Para la tasa de errores de la subcapa MAC, divida el número total de errores de la subcapa MAC por el número total de tramas. Para la tasa de las tramas de broadcast/multicast, divida el número total de broadcast/multicast por el número total de tramas.

	Promedio de Utilización de Red	Picos de Utilización de Red	Promedio de Tamaño de Tramas	Tasa de Errores CRC	Tasa de Errores de la Subcapa MAC	Tasa de Broadcast/Multicast
Segmento 1						
Segmento 2						
Segmento 3						
Segmento 4						
Segmento 5						

Tabla 6. Estadísticas de Monitoreo de Red.

4.1.3.9 Paso 9: *Caracterizando la Utilización de la Red.*

Configure la herramienta de monitoreo para obtener un promedio de las estadísticas de utilización de la red una vez cada hora para determinar cuando son las horas pico. Si la red está saturada (sobre utilizada), monitoree la utilización de la red cada minuto. Los picos sobre el 40% que se presenten durante los últimos minutos causan una notable degradación en el desempeño de la red.

Caracterice cuánto ancho de banda utiliza cada segmento de red por los diferentes protocolos, completando la tabla 7. Muchas herramientas de monitoreo permiten especificar el ancho de banda usado por los diferentes protocolos como ancho de banda absoluto o ancho de banda relativo.

Utilice las siguientes instrucciones para el llenado de la tabla:

- En el campo “Utilización de Red Relativa”, ingrese la cantidad del ancho de banda usado por cada protocolo en comparación con el ancho de banda total usado en ese segmento.
- En el campo “Utilización de Red Absoluta”, ingrese la cantidad del ancho de banda usado por cada protocolo en comparación con la capacidad total del segmento, por ejemplo, en comparación con 100 Mbps en Fast Ethernet.
- En el campo “Promedio del Tamaño de Trama”, ingrese el promedio del tamaño de trama para cada protocolo.
- En el campo “Tasa de Broadcast/Multicast” ingrese la tasa de broadcast/multicast para cada protocolo.

	Utilización de Red Relativa	Utilización de Red Absoluta	Promedio del Tamaño de Trama	Tasa de Broadcast/Multicast
IP				
IPX				
AppleTalk				
NetBIOS				
SNA				
Other				

Tabla 7. Utilización de Red.

Para más protocolos, puede configurar el monitoreo de la red, incluso para ver más allá de los datos. Por ejemplo, en un ambiente IP, es usual para conocer cuánto ancho de banda es utilizado por los protocolos de enrutamiento, aplicaciones basadas en TCP y aplicaciones basadas en UDP.

4.1.3.10 Paso 10: *Caracterizando el Estado de los Principales Enrutadores.*

Caracterizar el estado de los principales enrutadores en la red, completando la tabla 8. Planee esta actividad aproximadamente en un día, dependiendo del número de Enrutadores. Complete la siguiente tabla cada hora para cada interfaz como se muestra:

- En el campo “Nombre de Enrutador”, ingrese el nombre de cada enrutador principal.
- Para completar los siguientes campos, investigue con que comandos puede obtener los valores promedio para los “5 Minutos de Utilización del CPU”,

"Paquetes Tirados en la Cola de Salida por Hora", "Paquetes Tirados en la Cola de Entrada por Hora", "Paquetes Perdidos por Hora" y "Paquetes Ignorados por Hora".

- En el campo "Comentarios", ingrese cualquier comentario que ayude a caracterizar el estado de cada enrutador.

	Nombre de Enrutador	5 Minutos de Utilización del CPU	Paquetes Tirados en la Cola de Salida por Hora	Paquetes Tirados en la Cola de Entrada por Hora	Paquetes Perdidos por Hora	Paquetes Ignorados por Hora	Comentarios
Enrutador 1							
Enrutador 2							
Enrutador 3							
Enrutador 4							
Enrutador 5							

Tabla 8. Estado de los Enrutadores.

4.1.3.11 Paso 11: *Caracterizando las Herramientas y Sistemas de Administración de la Red Existente.*

Liste el tipo de plataformas y herramientas de administración de la red que se encuentren en uso. Si están disponibles, obtenga ejemplos recientes de reportes diarios, reportes semanales y reportes mensuales.

4.1.3.12 Paso 12: *Resuma la Salud del Interconexión Existente.*

Basado en los datos que obtuvo de la red, verifique cual de los siguientes elementos es verdadero. En una red saludable, debe verificar todos los elementos.

Note que los puntos son solo aproximaciones. Los umbrales exactos dependen del tráfico, aplicaciones, interconexiones de dispositivos, topología, y criterios para aceptar el desempeño de la red.

- Ningún segmento Ethernet se satura (no más del 40% de utilización de red).

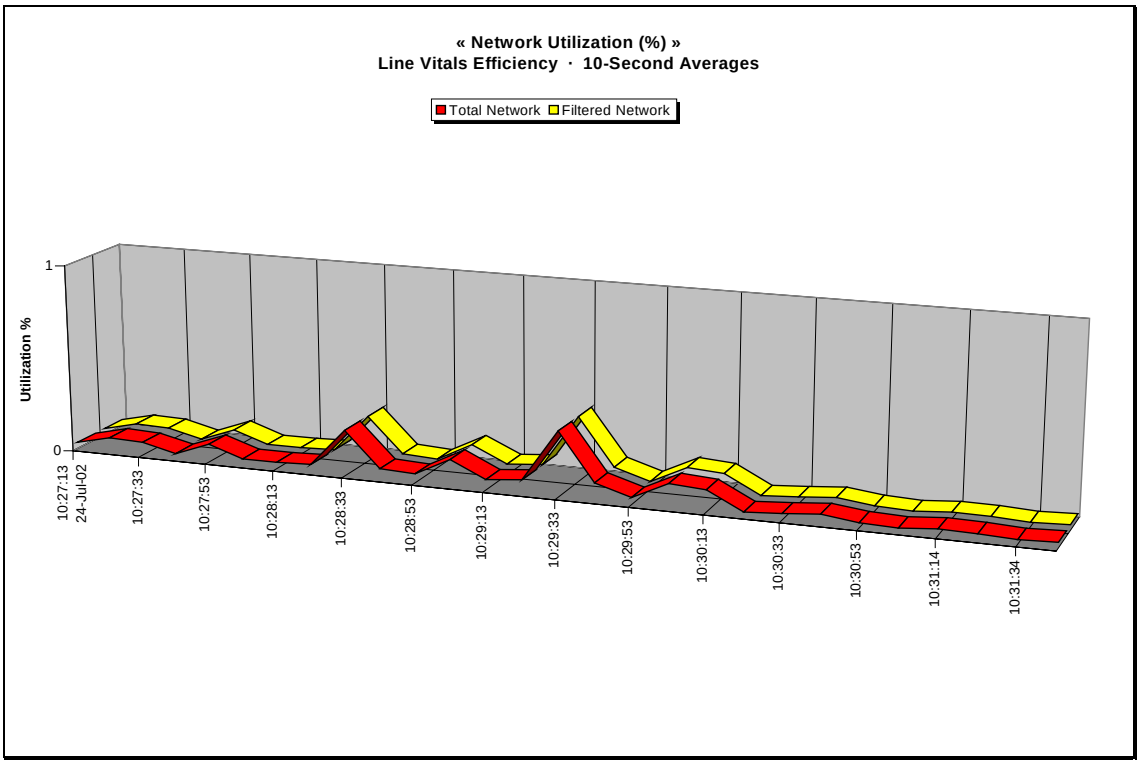


Figura 1. Utilización de red.

- Ningún enlace WAN está saturada (no más del 70% de utilización de red).

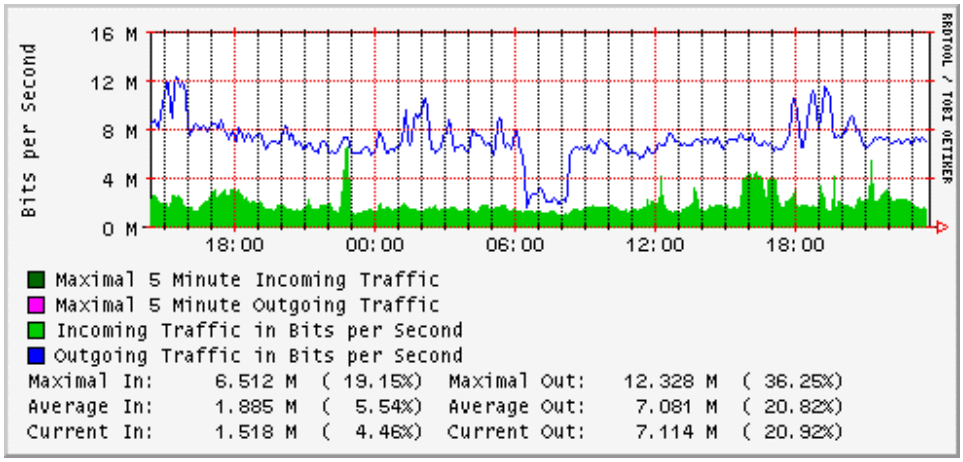


Figura 2. Análisis de tráfico en un enlace WAN de 34.368 Mbps (E3).

- El tiempo de respuesta es generalmente menor que 100 milisegundo (1/10 de un segundo).
- Ningún segmento tiene más del 20% de broadcast/multicast.

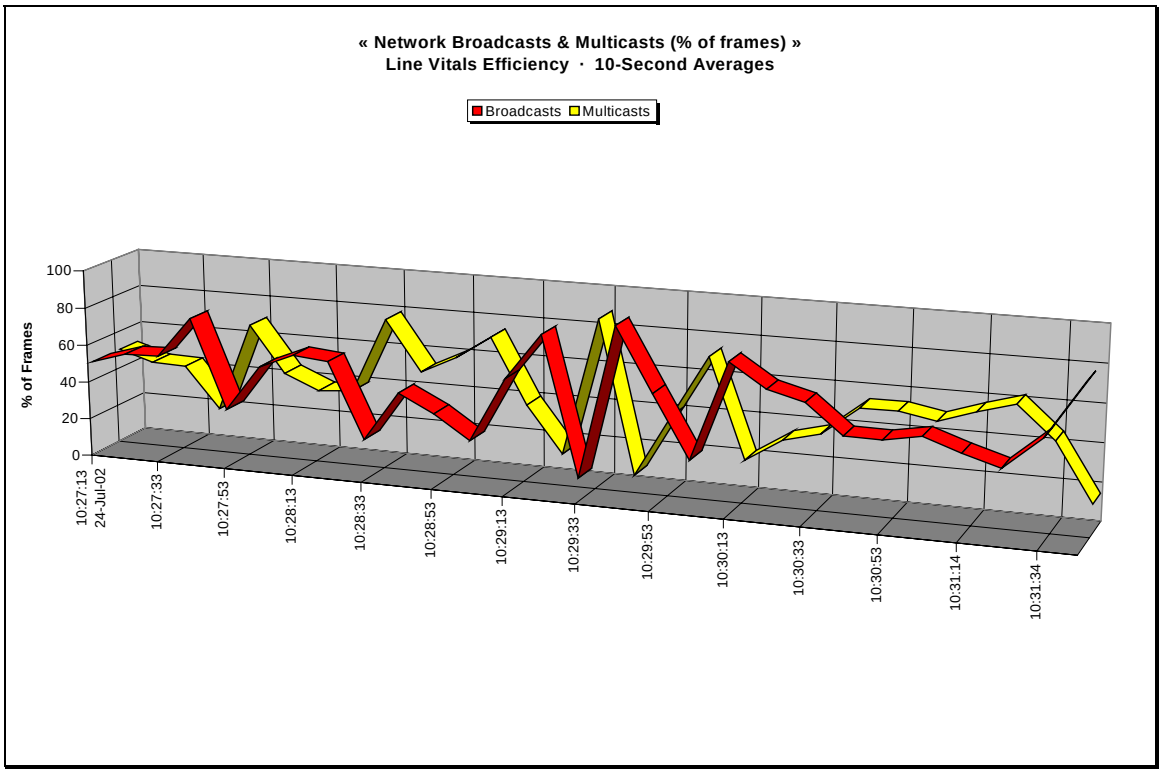


Figura 3. Porcentaje de tramas Multicast y de Broadcast.

- Los Enrutadores no son sobre utilizados (no más del 75% en 5 minutos de utilización del CPU).
- El número de paquetes tirados en la cola de salida, no excede más de 100 en una hora para cualquier enrutador (depende del fabricante).
- El número de paquetes tirados en la cola de entrada, no excede más de 50 en una hora para cualquier enrutador (depende del fabricante).
- El número de búfer perdidos, no excede más de 25 en una hora para cualquier enrutador (depende del fabricante).
- El número de paquetes ignorados, no excede más de 10 en una hora para cualquier enrutador (depende del fabricante).
- Ningún segmento tiene más de un error de CRC por millón de bytes de datos.
- Ningún segmento Ethernet, tiene más de 0.1% del resultado de los paquetes en las colisiones.

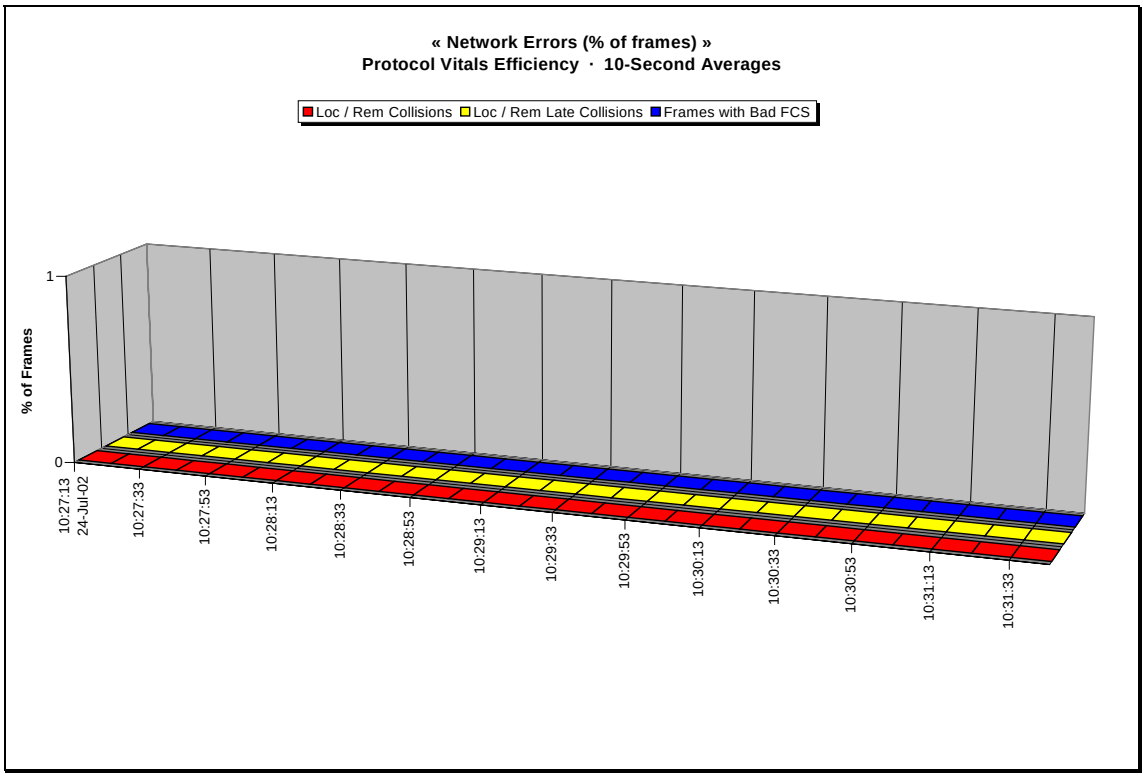


Figura 4. Porcentaje de errores de red.

Documente cualquier situación relacionada sobre la salud de la red existente y la habilidad con la que cuente para apoyar el crecimiento.

4.2 Obteniendo las nuevas necesidades.

4.2.1 Objetivos

- Determinar las necesidades del usuario para nuevas aplicaciones, protocolos, número de usuarios, uso en horas pico, y la administración de la red.
- Realizar el diagrama de flujo de la información para las nuevas aplicaciones.
- Aislar los criterios del usuario para aceptar el desempeño de la red.
- Listar algunas herramientas que ayudarán a caracterizar el nuevo tráfico en la red.
- Predecir la cantidad y el tipo de tráfico causado por las aplicaciones, basado en el tráfico típico de la red.

4.2.2 Determinando las Nuevas Necesidades de los Usuarios de la Red.

Determinar las necesidades de los usuarios para un nuevo diseño de red, es uno de los más importantes tareas en el diseño de la red. Esta sección provee paso por paso para

determinar esos requerimientos. Este camino asegurará el diseño de la red específicamente conociendo las necesidades de los usuarios. Haga una descripción de las ideas más importantes o hechos más importantes en el sitio donde se encuentren los usuarios y utilice esta información como un checklist.

Complete los siguientes pasos para determinar las necesidades de la red de los usuarios:

4.2.2.1 Paso 1: *Identifique las Limitantes del Negocio.*

- Documente el plan que muestre el presupuesto y los recursos que la empresa u organización estén dispuestos a gastar para el proyecto.
- Documente la línea del tiempo del proyecto, por ejemplo, una diagrama de Gantt.
- Identifique cualquier requerimiento del personal responsable de administrar y operar la red, como entrenamiento o contrataciones.

4.2.2.2 Paso 2: *Identifique los Requerimientos de Seguridad.*

- Juzgue los riesgos de seguridad y determine cuanta seguridad será necesaria y de que tipo.
- Determine los requerimientos de acceso de datos para usuarios no autorizados.
- Determine los requerimientos de autorización y autentificación para sucursales, usuarios móviles y usuarios remotos.
- Identifique cualquier requerimiento para autentificar rutas recibidas por enrutadores de acceso u otros enrutadores.
- Identifique cualquier requerimiento para la seguridad de hosts como seguridad física de los hosts, cuentas de usuarios, registro de software, los derechos de acceso a los datos, y así sucesivamente.

4.2.2.3 Paso 3: *Identifique los Requerimientos de Administración.*

- Aísle cualquier requerimiento para la administración predeterminada de la red.
- Aísle cualquier requerimiento para la razón de ser así la administración de esa red.
- Aísle cualquier requerimiento para la configuración de la administración de la red.
- Aísle cualquier requerimiento para el desempeño del proceso de administración de la red.
- Aísle cualquier requerimiento para la seguridad de la administración de la red.

4.2.2.4 Paso 4: *Obtenga los Requerimientos de Aplicaciones.*

- Documente los nombres y tipos de nuevas aplicaciones.
- Documente los nombres y tipos de nuevos protocolos.

- Documente el número de usuarios quienes usarán nuevas aplicaciones y protocolos.
- Haga el diagrama del flujo de información cuando se introducen nuevas aplicaciones.
- Identifique las horas pico del uso de nuevas aplicaciones.

4.2.2.5 Paso 5: *Caracterizando el Nuevo Tráfico de Red.*

- Caracterice la Carga del Tráfico.
- Caracterice el Tráfico Incluyendo:
  - Broadcast/Multicast, por ejemplo, figura 3.
  - Windowing y control de flujo.
  - Mecanismos de recuperación de errores.
  - Tamaños de trama soportados, por ejemplo, figura 5.

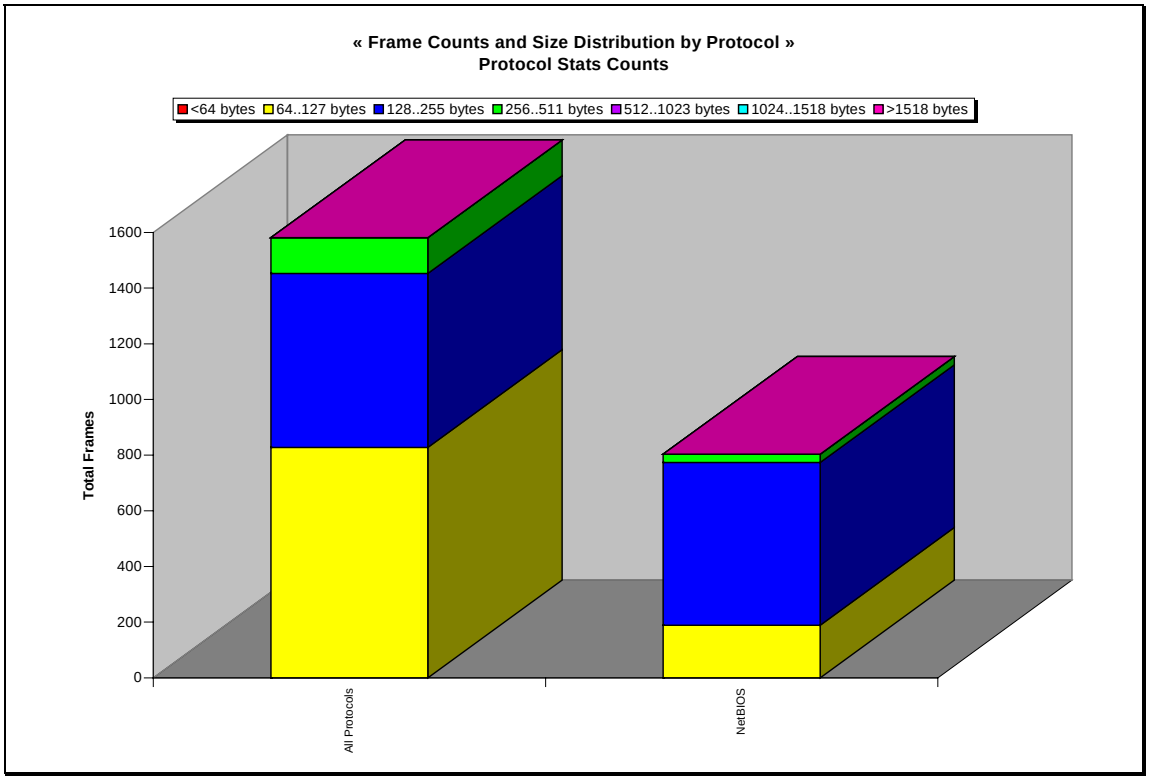


Figura 5. Conteo de tramas y distribución de tamaño por protocolo.

4.2.2.6 Paso 6: *Identifique los Requerimientos de Diseño.*

- Tiempo de Respuesta: La cantidad de tiempo para recibir una respuesta para una petición de servicio por el sistema de red.

- La Exactitud: El porcentaje de tráfico útil que se transmite correctamente en el sistema, relativamente al tráfico total, incluyendo la transmisión de errores.
- Disponibilidad: Cantidad de tiempo en el que está operando la red.
- Máxima utilización de Red: Máximo porcentaje de la capacidad total (ancho de banda) de un segmento de red que puede ser usado antes de que la red se considere "saturada".
- Throughput: Calidad de los datos transmitidos correctamente entre nodos por unidad de tiempo, usualmente en segundos.
- Eficiencia: Es el proceso de medición de cuánto esfuerzo se requiere para producir una cierta cantidad de throughput de datos.
- Latencia (o retardo): Tiempo entre una trama lista para la transmisión de un nodo y la realización de la trama de la transmisión exitosa.

Una vez caracterizada la red y habiendo extraído todos los requerimientos, elabore un documento que especifique las necesidades de los usuarios. El documento de necesidades deberá resumir los datos recolectados. Usa el documento para establecer consensos con los usuarios acerca de sus necesidades.

4.3 Diseño de la Topología de red.

Todo diseño de topología está basado en el modelo de referencia OSI, ya que ahí tenemos la capa de red. Existen diferentes tipos de modelos para el diseño de la topología, y la selección estará determinada por las necesidades de los usuarios de la red, el costo y la disponibilidad. Nosotros hemos descrito varios modelos en el capítulo 3 donde se describen las características de cada modelo, y que de acuerdo con éstas y la caracterización de la red o las necesidades, se utilizará un modelo o incluso varios.

Conforme avancemos en este capítulo contaremos con más fundamentos para seleccionar dicho modelo.

4.4 Provisión de Hardware y medios de comunicación LAN.

4.4.1 Objetivos

- Reconocer la escalabilidad de las limitantes y problemas para una tecnología LAN estándar.
- Seleccionar la tecnología LAN que cubra las necesidades de desempeño, capacidad y escalabilidad de los usuarios de la red requieren en redes pequeñas a medianas.
- Identificar cómo revisar un diagrama de topología de red de alto nivel para incluir hardware y medios de comunicación.

4.4.2 Evolución de Servicios de Capa 2 y Capa 3.

La capa 2, también conocida como capa de enlace, opera dentro de una especificación LAN o segmento WAN. En los últimos dos años, las LANs se han revolucionado rápidamente por el creciente uso de Switches capa 2. Las compañías están

reemplazando Hubs por Switches a pasos gigantescos. Los Switches LAN proveen mejoras de desempeño para nuevas y existentes aplicaciones en la red aumentando el ancho de banda, y el throughput para grupos de trabajo y servidores locales.

La capa 3, también conocida como capa de red, opera entre y a través de los paquetes. Protocolos como Internet Protocol (IP), Internetwork Packet Exchange (IPX) y AppleTalk´s Datagram Delivery Protocol (DDP) operan en la capa 3. En la WAN, la capa 3 permite la interconexión de sucursales o sitios remotos para construir una red de datos global. Como un ejemplo, la red global Internet está basada en la tecnología de capa 3.

El establecimiento de una red de capa 3, implantada con enrutamiento e interconexión con Switches, provee servicios como seguridad, opciones de calidad de servicio (QoS, Quality Of Service) y administración del tráfico. El enrutamiento, provee el control necesario para construir redes funcionales y escalables.

Tradicionalmente, el switcheo de capa 2 había sido provisto por LAN Switches, y la interconexión de capa 3 había sido provista por los Enrutadores. Cada vez más, esas dos funciones de red se integran en las mismas plataformas. Habrá una amplia gama de plataformas proveyendo diferentes desempeños y rangos de capacidades para cada función de red, pero los usuarios ganarán ventajas fundamentales para la integración de las capas. Los usuarios serán capaces de reducir el número de dispositivos de interconexión que necesitan ser comprados, instalados, soportados y mantenidos. Además, los usuarios podrán aplicar eficientemente servicios de la capa 3, como seguridad y capacidades de QoS, para específicos usuarios individuales y aplicaciones.

Reflejo de la integración de la tecnología de capa 3 dentro de dispositivos LAN Switching, el equipo WAN Switching incorporará probablemente cada vez más capacidades de interconexión de capa 3. Como los tradicionales enrutadores de capa 3, ganan soporte para una alta capacidad y ancho de banda, la integración de tecnologías de capa 2, permitirá a los enrutadores lograr niveles óptimos de desempeño, densidad de puertos, y costo-eficacia.

4.4.3 Resolviendo Problemas con la Interconexión.

La decisión para usar un dispositivo de interconexión depende de que problemas se estén tratando de resolver. Los problemas existentes en una red pueden ser clasificados como sigue:

- **Problemas de Medios**
  Los problemas de medios son referidos a un excesivo número de colisiones en Ethernet. Los problemas de medios son causados por muchos dispositivos, todos con una alta carga para el segmento de red. Los problemas de medios pueden ser resueltos dividiendo una red en segmentos más pequeños utilizando VLANs.

- **Problemas de Protocolos**
  Los problemas de protocolos son causados por protocolos que no son bien escalados, por ejemplo, protocolos que envían un excesivo número de broadcast. Los problemas de protocolos pueden ser resueltos dividiendo una red en segmentos usando enrutadores o creando VLANs por protocolo.

- **Necesidad para Transportar Payloads más Grandes**
  Esta categoría incluye la necesidad para ofrecer servicios de voz y video a través de la red. Esos servicios requieren mucho más ancho de banda que la que está disponible, seguramente, en la red actual. Los problemas de transporte pueden ser solucionados utilizando una tecnología con alto ancho de banda, como Gigabit Ethernet.

4.4.4 Switching versus Enrutamiento en el Diseño de Red.

La decisión de usar enrutadores o switches depende del problema en cuestión (issue). Cuando se prueban dispositivos de interconexión de pequeñas a medianos tamaños de redes, es necesario decidir cuando son apropiados los LAN switches y cuando son apropiados los enrutadores. En general, incorpore switches en pequeños a medianos diseños de redes para proveer las ventajas listadas:

- Alto ancho de banda en redes crecientes.
- Bajo costo por puerto para incrementar el ancho de banda para soportar nuevas aplicaciones.
- Fácil configuración y administración.
- Minimizar colisiones.

Si es necesario la interconexión de servicios, entonces los enrutadores son necesarios:

- Segmentan la red en dominios de broadcast individuales.
- Proveen reenvío inteligente de paquetes.
- Soportan caminos de red redundantes.
- Provee seguridad, políticas y administración de la red.
- Ofrecen manejabilidad, control y acceso WAN.

Cuando se utilizan switches, cada host asociado con un puerto es un dominio de ancho de banda. En el caso de un switch Ethernet, un dominio de ancho de banda es también conocido como dominio de colisión.

Todos los hosts dentro de un dominio de ancho de banda compiten por el mismo recurso de ancho de banda LAN. Todo el tráfico para cualquier host en el dominio de ancho de banda es visible para todos los otros hosts. En el caso de un dominio de colisión Ethernet, dos hosts el hecho de transmitir al mismo tiempo produce una colisión.

Un dominio de broadcast incluye todo el tráfico asociado con un puerto en un enrutador. Todo broadcast generado por cualquier host en el mismo dominio de broadcast es visible por todos los demás hosts que estén en el mismo dominio de broadcast. Los protocolos utilizados por los hosts, tal como, AppleTalk, NetBIOS, IPX e IP requieren el uso de broadcast y multicast para descubrir recursos y propagar anuncios. Los switches reenvían broadcast y multicast, mientras que los enrutadores no reenvían broadcast.

La radiación de broadcast se refiere al camino que el broadcast y multicast radie por el host origen para todos los hosts conectados en la misma LAN, causando que todos los hosts en la LAN hagan un extra proceso. Cuando el broadcast y multicast es más que el 20% del tráfico en la red LAN, el desempeño es degradado.

4.5 Diseño del modelo de nombres y el modelo de direccionamiento de red.

4.5.1 Objetivos

- Identificar los pasos o procesos requeridos para diseñar un modelo de direccionamiento de red.
- Proponer un modelo de direccionamiento para redes, subredes y hosts que proveen escalabilidad.
- Proponer un esquema de nombres para servidores, enrutadores y hosts.

4.5.2 Modelo de Direccionamiento

Diseñar el modelo de direccionamiento de red y el modelo de nombres, es una de las tareas más importantes en el diseño de interconexión. Esto es posible realizarlo con la selección de un protocolo de enrutamiento.

Para diseñar un modelo de direccionamiento de red y el modelo de nombres, son recomendables los siguientes pasos:

Paso 1. Diseñe una jerarquía para el direccionamiento de sistemas autónomos, áreas, redes, subredes y hosts.

Paso 2. Diseñe la sumarización de rutas (agregación).

Paso 3. Diseñe un plan para distribuir la autoridad administrativa para el direccionamiento y el modelo de nombres a los más bajos niveles de jerarquía.

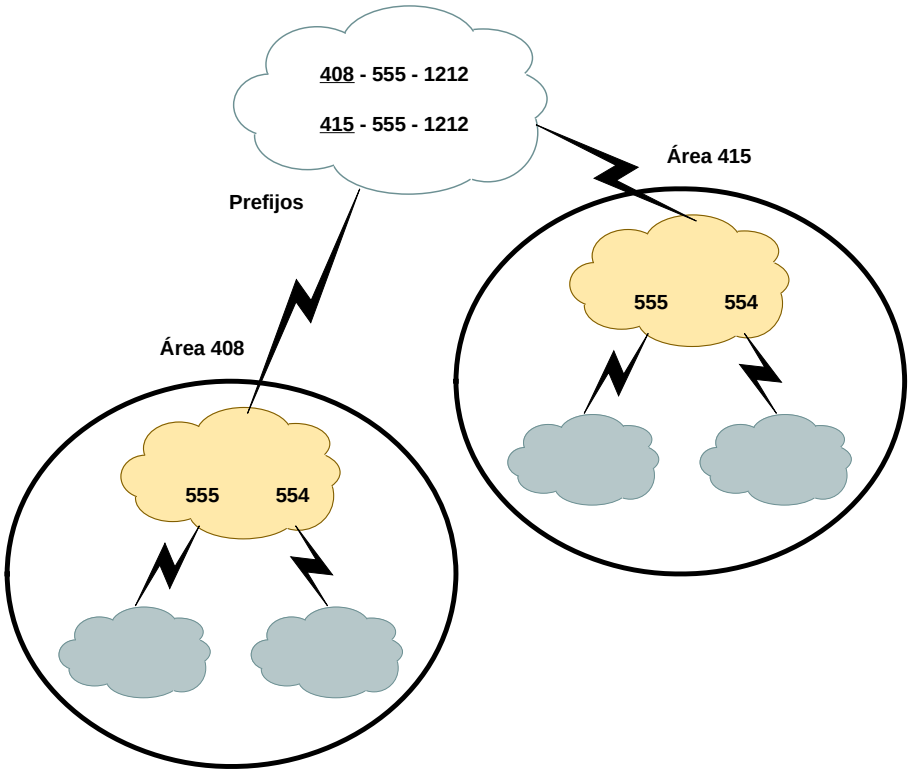


Figura 6. Diagrama de la jerarquía del direccionamiento de red

Paso 4. Diseñe un método para el mapeo de locaciones geográficas para el número de redes.

Paso 5. Desarrolle un plan para identificar hosts especiales, como enrutadores y servidores con específicos identificadores de nodos (node IDs).

Paso 6. Desarrolle un plan para configurar el direccionamiento de red en hosts de usuarios finales, puedes elegir entre el direccionamiento dinámico o estático. Sin embargo, cabe señalar que si utiliza direccionamiento dinámico será necesario utilizar algún método de autentificación a nivel de acceso para evitar usuarios no autorizados en la red.

Paso 7. También se recomienda desarrollar un plan para el uso de gateways para mapear el direccionamiento privado a direccionamiento público:

- NAT (Network Address Translation) es usado con el siguiente direccionamiento como lo especifica el RFC 1918:

10.0.0.0 a 10.255.255.255
172.16.0.0 a 172.31.255.255
192.168.0.0 a 192.168.255.255

Paso 8. Diseñe un esquema para los nombres de los servidores, enrutadores y hosts de usuarios finales:

- Los nombres deben tener un significado para facilitar el troubleshooting (diagnóstico y solución de un problema), por ejemplo, para los nombres de hosts de usuarios finales:

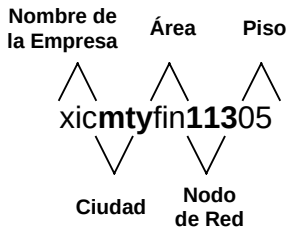


Figura 7. Propuesta de un esquema de nombres para hosts de usuarios finales.

- Para nombres de dispositivos en ambientes IP, instale y configure un servidor de DNS.

4.5.2.1 Direccionamiento IP

Las direcciones IP usadas por organizaciones son susceptibles a cambios por una variedad de razones, incluyendo las siguientes:

- Reorganización de la empresa o institución.
- Movimiento físico del equipo.
- Nueva estrategia de relaciones.
- Cambios en el o de ISP.
- Nuevas aplicaciones.
- Necesidades de una conectividad de Internet global.
- Implantación de subredes.

Cuando diseñe el direccionamiento IP, es importante diseñar el direccionamiento de red para soportar subneteo.

El subneteo reduce el número de rutas en la tabla de enrutamiento, tráfico por la actualización de rutas, y sobretodo el encabezado de enrutamiento. Reducir el tráfico por la actualización de las tablas de enrutamiento puede ser muy importante en líneas de baja velocidad.

La arquitectura telefónica ha sido manejada con prefijos de enrutamiento por muchos años. Un teléfono conmutado en la Ciudad de México no necesita conocer como alcanzar una línea específica en Monterrey. Solamente necesita reconocer que la llamada no es local. Un proveedor de servicios de telefonía de larga distancia necesita reconocer que el 55 es para la Ciudad de México pero no necesita saber los detalles de cómo alcanzar la línea específica en la Ciudad de México.

El prefijo de enrutamiento no es nuevo en ambientes IP. Un enrutador necesita saber solamente como alcanzar el siguiente salto (next hop), pero el enrutador no necesita saber los detalles de cómo alcanzar un host final que no es local.

Como en el ejemplo de la línea telefónica, los enrutadores IP hacen decisiones jerárquicas. Una dirección IP incluye una parte de prefijo y una parte de host. Los enrutadores usan el prefijo para determinar el camino para una dirección destino que no es local. La parte del host es usada para alcanzar al host local.

Un prefijo identifica un bloque de número de hosts y es usado para enrutar para ese bloque. De acuerdo con el RFC 1518 un prefijo es una dirección IP y alguna indicación de los bits contiguos más significativos hacia la izquierda dentro de esa dirección. La indicación de los bits contiguos más significativos hacia la izquierda han sido tradicionalmente hechos con una indicación de la clase de red y una máscara de red predeterminada, por ejemplo, 8. Sin embargo, esto ya no es correcto utilizarlo o mencionarlo, una indicación de longitud correcta ahora es una dirección de red seguida de una diagonal (slash) y el número de bits de la máscara de red, por ejemplo, 200.77.231.142/28.

Como un ejemplo, suponga que un enrutador tiene las siguientes redes detrás de él:

- 192.108.168.0
- 192.108.169.0
- 192.108.170.0
- 192.108.171.0
- 192.108.172.0
- 192.108.173.0
- 192.108.174.0
- 192.108.175.0

Este enrutador puede anunciar solamente una red: 192.108.168.0/21.
Anunciando esta sola red, el enrutador está diciendo “enruto los paquetes hacia me si el destino tiene los primeros 21 bits puestos a 192.108.168”.

En binario, los 21 bits son como sigue (x es un valor binario; no importa que valor pueda tomar):

- 1100 0000 (el primer octeto = 192)
- 0110 1100 (el segundo octeto = 108)
- 1010 1xxx (el tercer octeto empieza con 10101, el cual es 168 en decimal)
- xxxx xxxx (el cuarto octeto puede ser cualquiera)

Si convierte las redes listadas de decimal a binario, se dará cuenta que todas ellas comienzan con los mismos 21 bits: 1100 0000 0110 1100 1010 1xxx.

4.6 Seleccionando protocolos de enrutamiento y bridging.

4.6.1 Objetivos

➢ Identifique las ventajas y problemas de los protocolos de enrutamiento, y protocolos de bridging.
➢ Recomendar protocolos de enrutamiento y bridging que cubran requerimientos específicos para desempeño, seguridad y capacidad.

Los protocolos de enrutamiento pueden ser caracterizados por qué información es intercambiada entre los routing peers. Los protocolos pueden:

- Enviar actualizaciones periódicas
- Tiene un mecanismo separado de Hello
- Intercambian información acerca de enlaces
- Intercambian información acerca de rutas

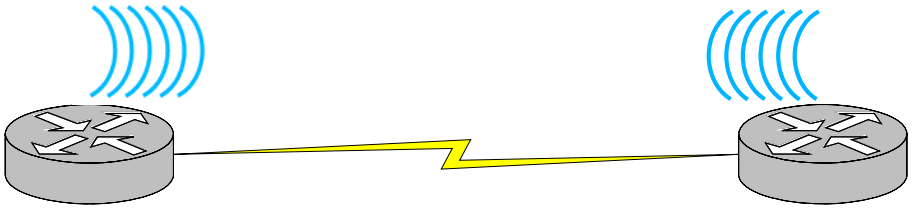


Figura 8. Intercambio de información entre enrutadores.

Las ventajas de los protocolos de enrutamiento pueden ser caracterizadas como sigue:

- Envío de actualizaciones periódicas
- Mecanismos de reconocimiento (Hello) separados
- Intercambio de información acerca de los enlaces
- Intercambio de información acerca de rutas

4.6.2 Limitantes de la Escalabilidad de los Protocolos de Enrutamiento

Los limitantes de la escalabilidad de los protocolos de enrutamiento, pueden ser caracterizados de la siguiente manera:

Limitantes en las métricas. Por ejemplo, una interconexión no basada en RIP puede tener un diámetro superior que 15 saltos.

Tiempo de convergencia. Convergencia es el tiempo que le toma a los enrutadores llegar a un entendimiento consistente de la topología de interconexión, después de un cambio en la red de topología. Los paquetes no pueden ser enrutados confiablemente hasta que se ha dado la convergencia de la topología. La convergencia es una limitante en el diseño para algunas aplicaciones. Por ejemplo, la convergencia es crítica cuando una aplicación

basada en tiempo real, se transporta en paquetes IP. La convergencia depende de los siguientes puntos:

- Medidores de tiempo (*timers*)
- Complejidad y diámetro de la red
- Frecuencia de la actualización de los protocolos de enrutamiento
- Características de los protocolos de enrutamiento

La convergencia tiene dos componentes:

- El tiempo que le toma detectar una falla en el enlace
- El tiempo para determinar una nueva ruta

4.6.3 Consideraciones de Uso de los Protocolos de Enrutamiento

Para seleccionar el protocolo de enrutamiento, conteste las siguientes preguntas:

- ¿Qué tan a menudo son transmitidas las actualizaciones de enrutamiento?
  - Es una función de la actualización de los medidores de tiempo
  - Las actualizaciones serán disparadas (triggered) por evento
- ¿Qué cantidad de datos son transmitidos (la tabla de enrutamiento completa o solo algunos cambios de ella)?
- ¿Cuál es la amplitud de la distribución de las actualizaciones de enrutamiento?
  - Para los vecinos (neighbors)
  - Para el área de frontera
  - Para todos los enrutadores en el Sistema Autónomo (AS, Autonomous System)
- ¿Cómo son usadas las rutas estáticas y las rutas predeterminadas (default route)?
- ¿Es soportado el subneteo y cómo?

4.6.4 Protocolos de Bridging

Hay diferentes tipos de protocolos bridging, y se enlistan a continuación:

- Bridging Transparente (Transparent Bridging) es encontrado principalmente en ambientes Ethernet.
- Bridging Ruta-Fuente (Source-Route Bridging) es encontrado principalmente en ambientes Token Ring.
- Bridging de Traducción (Translational Bridging) intenta traducir de Bridging Ethernet a Bridging Token Ring.

- Bridging de Encapsulamiento (Encapsulating Bridging) permite a las tramas pasar en forma de paquetes a través del backbone de la red.
- Bridging Transparente de Ruta Fuente (Source-Route Transparent Bridging) permite a un bridge realizar las funciones de Bridge Transparente y de Fuente de Enrutamiento.

4.6.5 Problemas de Escalabilidad del Bridging Transparente

Un bridge en modo transparente envía hacia todos los puertos tramas multicast y broadcast, y tramas con dirección destino desconocida excepto por el puerto donde la trama fue recibida.

En el caso de las direcciones desconocidas, un bridge en modo transparente censa todas tramas y aprende cual puerto usar para alcanzar un dispositivo. También, aprende buscando en la dirección origen de todas las tramas, así que una dirección desconocida se convierte en una dirección conocida una vez que el dispositivo ha enviado una trama. La escalabilidad es un problema si el bridge tiene un número muy limitado de direcciones que puede aprender.

Los bridges en modo transparente implantan el algoritmo spanning-tree, la cual es especificada en IEEE 802.1d. El estado del algoritmo de spanning-tree que hay uno y solo un camino activo entre dos estaciones. El algoritmo se encarga de los loops deshabilitando los puertos del bridge. Los bridges en modo transparente envían tramas BPDU (Bridge Protocol Data Unit, Unidad de Datos del Protocolo Bridge) a nosotros para construir y mantener un spanning-tree. Spanning-tree tiene un *root bridge* y una configuración de los puertos activos en el bridge, seleccionados para determinar el camino con menor *costo* para el *root bridge*. Las tramas BPDU son enviadas para una dirección multicast cada dos segundos. La cantidad de tráfico causado por tramas BPDU puede ser un gran problema de escalabilidad, es lo mismo para todas las redes con numerosos switches o bridges, y no cambia.

4.6.6 Problemas de Escalabilidad del Bridging Ruta-Fuente

Con bridging ruta-fuente, un nodo origen encuentra a otro nodo por la exploración de envío de tramas. La escalabilidad es afectada por el tipo de exploración de tramas que el nodo origen envía. Una exploración de tramas puede ser una de las siguientes:

- **Exploración de todas las rutas**
  El nodo origen especifica que la exploración de tramas debe de tomar todos los posibles caminos. El nodo origen especifica usualmente que la respuesta debe tomar solo un camino de regreso.

- **Exploración de una ruta**
  El nodo origen especifica que la exploración de tramas debe de tomar solamente un camino, y que la respuesta debe tomar todos los caminos o solo uno para regresar.

Cuando la exploración de tramas de una ruta es usada, los bridges pueden usar el algoritmo sapnning-tree para determinar un solo camino para el destino. Si el algoritmo sapnning-tree no es usado, el administrador de la red debe seleccionar manualmente cual bridge debe reenviar la exploración de una ruta cuando hay múltiple redundancia de conexión de bridges.

4.7 Seleccionando una estrategia de administración de red.

4.7.1 Objetivos

- Recomendar protocolos que reúnen los requisitos para al administración de una red.
- Describir los pasos que deben tomarse para desarrollar una estrategia de administración de red.

4.7.2 Las Metas de la Administración de Red

Como las interconexiones de redes crecen en alcance y complejidad, las capacidades de administración de red robustas se convierten cada vez más importantes. Muchas organizaciones requieren un ancho rango de funciones de administración de red para ayudarse a maximizar la disponibilidad de aplicaciones críticas y minimizar el sobre costo de la propiedad. En general, muchas organizaciones tienen las siguientes metas para los productos de administración de sus redes y estrategias:

- Conectividad
- Seguridad
- Optimización de costos
- Crecimiento manejable

4.7.3 Procesos de la Administración de Red

Aunque las metas para la administración de la red pueden ser simplemente declaradas, entender todas las tareas requeridas para conocer las metas es difícil. Las tareas de administración de red pueden ser divididas en tres áreas principales:

- Monitoreo y diagnóstico
- Diseño y optimización
- Implantación y cambios

Monitoreo y diagnóstico	Diseño y optimización	Implantación y cambios
• Definir umbrales • Excepciones de monitoreo • Aislar problemas • Validar problemas • Solución de problemas (*troubleshooting*) • Desviación de problemas	• Colección de datos • Creación *baseline* (línea base) • Tendencia del análisis • El análisis del tiempo de respuesta • Planeación de capacidades • Procuración • Diseño de topología	• Instalación • Configuración • Administración del direccionamiento • Agregar, mover, cambios • Administración de la seguridad • Administrador del proyecto (*Project Manager*) • Administración de inventario y recursos • Administración de usuarios • Administración de datos

Tabla 9. Procesos de la Administración de Red.

4.7.4 Administración Proactiva de Red

Muchas administraciones de red son reactivas, aunque la industria se está moviendo hacia un acercamiento proactivo para la administración de las redes. Muchos vendedores de equipo de redes de datos se han estado animando a una administración proactiva de la red por años, debido a la reducción del personal operativo y la falta de capacitación al personal existente en las empresas, profesionales de las redes han requerido disponer de su tiempo para implantar cambios y solucionar problemas. Sin embargo, las empresas reconocen la importancia de la estrategia de la interconexión de sus redes, más énfasis está siendo puesto en la administración de red proactiva.

La administración proactiva de una red significa el monitoreo de la red incluso cuando ésta no tenga ningún problema. Esto significa:

- Colección de estadísticas y tendencias de monitoreo.
- Pruebas rutinarias controladas, como las medidas de tiempo de respuesta.
- El tiempo asignado por lo menos una vez al mes para concentrar las estadísticas y realizar un informe básico que describe el estado actual de la red.
- Definiendo las metas de servicio para la red, por ejemplo, aceptable tiempo fuera de servicio, tiempo de respuesta, throughput, facilidad de uso y escalabilidad.
- Realizar reportes de la calidad de servicio que ha sido entregada en el último mes.

4.7.4.1 Desarrollando Estrategias de Administración Proactiva de Red

Para ayudar a desarrollar una estrategia de administración proactiva de la red sigue los pasos de abajo:

- Determinar las metas de los servicios de red
- Definir métricas para medir si se han alcanzado las metas

- Definir procesos para la colección de datos y reporteo
- Implantar sistemas de administración de red
- Colecciona datos de desempeño y tendencias de los registros acumulados
- Analiza los resultados y genera reportes
- Ubica irregularidades y cuellos de botella en la red
- Planea e implanta mejoras en la red
- Revisa y ajusta métricas y procesos si es necesario
- Controla y documenta los cambios

4.7.5 Monitoreo Remoto

La norma SNMP (Simple Network Management Protocol, Protocolo de Administración de Red Simple) Remote Monitoring (RMON) permite monitorear paquetes y patrones de tráfico en segmentos LAN. RMON:

- Número de paquetes
- Tamaño de paquetes
- Broadcast
- Utilización de red
- Errores y condiciones como colisiones en Ethernet
- Estadísticas para hosts, incluyendo generación de errores por hosts, el host más ocupado, y que hosts hablan con que hosts.

Las características de RMON incluyen vistas históricas de estadísticas RMON basadas en intervalos de muestreo de usuarios definidos, alarmas basadas en umbrales de usuarios definidos, y captura de paquetes basadas en filtros de usuarios definidos.

RMON es definido como una porción de MIB II (Management Information Data Base, Base de Datos de la Información de Administración). El RFC 1757 define los objetos para una administración remota de dispositivos de red.

La especificación RMON comprende nueve grupos de administración de objetos. Los agentes de RMON pueden implantar algunos o todos los siguientes grupos:

- Estadísticas
- Historial
- Alarmas
- Hosts
- Top “n” de hosts
- Matriz de tráfico
- Filtros
- Captura de paquetes
- Eventos

4.8 Documento de diseño.

4.8.1 Objetivo

- Escribir un documento de diseño o una respuesta al requerimiento de diseño.

4.8.2 Contenido del Documento de Diseño

La sección de requerimiento de diseño resume las conclusiones como resultado de identificar las necesidades en una red. Debe incluir:

- Caracterización de la red existente, incluyendo:
    - Descripción de la red existente, incluyendo un diagrama de la topología
    - Aplicaciones actuales, protocolos, topología, y el número de usuarios
    - Problemas relevantes de negocio para el proyecto de diseño de la red
- Requerimientos del usuario:
    - Requerimientos para el desempeño, seguridad, capacidad, y escalabilidad para soportar nuevas aplicaciones
    - Flujo de información para nuevas aplicaciones

En la sección de la solución del diseño, describe la solución recomendada, y las características y beneficios que éste provee. Organiza el contenido en esta sección de acuerdo a las necesidades del usuario, lista en orden las prioridades del usuario. Asegúrate de incluir los siguientes componentes:

- Propósito de la topología de red, incluyendo un diagrama de la topología de red y las ventajas ofrecidas por el diseño de la topología de red.
- Hardware y medios recomendados para la LAN, incluye características y beneficios de cada componente que se seleccionó, relacionado a las necesidades del usuario de desempeño, seguridad, capacidad y escalabilidad.
- Hardware y medios recomendados para la WAN, incluye características y beneficios y beneficios de cada componente seleccionado, relacionado a las necesidades del usuario de desempeño, seguridad, capacidad y escalabilidad.
- Modelo de nombres y el modelo de direccionamiento de red, incluye el modelo de direccionamiento y de nombres para todos los componentes de la red, relacionado a las necesidades del usuario de desempeño, seguridad, capacidad y escalabilidad.
- Protocolos recomendados de enrutamiento y bridging de la red, incluye los protocolos recomendados de enrutamiento y bridging, relacionado a las necesidades del usuario de desempeño, seguridad, capacidad y escalabilidad.
- Características del software provisto para la red, incluye las características del software, políticas de seguridad, como listas de acceso, autentificación, servicios proxy, encriptación, compresión, encolamiento, etc. Relacionados con las características del software seleccionado para las necesidades del usuario de desempeño, seguridad, capacidad y escalabilidad.

- Estrategia de administración de red, incluye los productos recomendados y los protocolos relacionados con las necesidades del usuario. Incluya una descripción de la estrategia de administración proactiva de red.

El resumen de la solución y artículos de cómo la solución resuelve las necesidades del usuario. Puede incluir apéndices que contengan información adicional. Incluya tantos apéndices como sea necesario para detallar la información. Asegúrese de realizar el documento con un lenguaje claro para que el usuario lea y comprenda. Es decir, tenga en mente el umbral del usuario para aceptar grandes cantidades de información. Los apéndices pueden incluir:

- Una lista de contactos del proveedor y de la empresa del cliente (usuario).
- Una línea de tiempo de la implantación del proyecto (plan de trabajo).
- Información adicional de los productos utilizados para el proyecto (ficha técnica).
- Detalles del direccionamiento y el esquema de nombres que se desarrollo para el usuario.
- Detalles para la estrategia de administración de la red que se desarrollo para el usuario.
- Resultados del prototipo de pruebas.
- El resultado de cualquier medida de desempeño que hayas realizado en la red del usuario.

4.9 Validando el diseño de red.

4.9.1 Objetivos

- Determine cuanta de la estructura de red debe ser construida para proveer para que el diseño de red cumpla con las necesidades del usuario.
- Liste las tareas requeridas para construir el prototipo o piloto.
- Describa como demostrar el prototipo o piloto al usuario.

4.9.2 Pasos para Construir un Prototipo

Paso 1. Determinar cuanta de la estructura de red debe ser construida para proveer para que el diseño de red cumpla con las necesidades del usuario. Investigue los servicios y herramientas que puedes usar para simplificar las tareas de compra, instalación y configuración del equipo para el prototipo, por ejemplo, probando servicios y herramientas de simulación de red.

Paso 2. Desarrolle un plan de prueba:

- Realice un diagrama de la topología del ambiente de prueba. Incluye en el diagrama los parámetros de mayor configuración:
  - Liste las herramientas de simulación, del hardware y software que necesitarás para el prototipo.

- Incluya cables, módems, conexiones WAN, accesos de Internet, estaciones de trabajo, servidores, herramientas de simulación de diseño, simulador de equipos de telefonía y así sucesivamente.

- Liste y planee para cualquier otro recurso que puedas necesitar:

  - Programe el laboratorio en el sitio del usuario.
  - Ayude para trabajar con el personal del cliente (usuario).

- Desarrolle una lista de las pruebas y demostraciones que realizará:

  - Explique como cada prueba será realizada para que el diseño reúna las necesidades del usuario.

- Escriba un script para cada prueba o demostración:

  - Liste los pasos para proveer el diseño.
  - Describa como evitar fallas.

Paso 3. Configure y compre (si es necesario):

- Herramientas de simulación de red
- Hardware y software

Paso 4. Practicar la demostración.

Paso 5. Dirigir pruebas finales y demostraciones.

4.9.3 Pasos para Construir un Piloto

Para organizaciones pequeñas, un piloto puede ser más práctico. Un piloto es simplemente un diseño pequeño de un prototipo usado para demostrar funciones básicas.

Si aplica, hay recomendaciones mínimas para un diseño piloto:

Paso 1. Pruebe el diseño. Asegúrese que pueda reunir los requerimientos del usuario. Por ejemplo, los usuarios deberán ver sus pantallas dentro de un décimo de segundo.

Paso 2. Escriba un script para demostrar los resultados de la prueba:

- Asegúrese que las pruebas resulten como el diseño establece para que cubra las necesidades del usuario.

Paso 3. Practique la demostración.

Paso 4. Agende el tiempo con el usuario y presenta la demostración.

4.9.4 Usando un Analizador de Protocolos

Para utilizar el analizador de protocolos, asegúrese de tener el analizador de protocolos adjunto al medio a probar, si es un medio WAN de 10 Mbps ó 100 Mbps, Ethernet, o cualquier otro medio, Si es necesario configura el analizador de protocolos para el medio. Para analizadores WAN, a menudo es necesario especificar la capa del enlace de datos, si es HDLC, si es PPP, o un formato propietario, y así sucesivamente.

Asumiendo que el prototipo de red está instalado y que los usuarios de la red están ejecutando sus aplicaciones apropiadas, use el analizador de protocolos para:

- Capture datos por al menos un día.
- Identifique errores e irregularidades.
- Revise el porcentaje de utilización de red.
- Determine que porcentaje del tráfico es broadcast o multicast.

Para verificar que no hay problemas, utilice el Checklist para la Salud de la Red que se muestra más adelante.

También puede utilizar el analizador de protocolos para generar tráfico cuando se esté probando el prototipo o piloto. Si esto es impráctico para comprar, instale y configure todos los dispositivos requeridos para hacer un simulación real, también puede adquirir un subconjunto del analizador de protocolos y generar el tráfico para causar que la carga pueda ser presentada si todos los dispositivos fueran instalados. Esta simulación dará una aproximación del desempeño de la red, aunque no una vista exacta del desempeño actual que se espera.

Si a el usuario le preocupa la seguridad y el prototipo implanta una lista de acceso, use el analizador de protocolos para demostrar que el tráfico filtrado está trabajando correctamente. Por ejemplo, si la red A no debe alcanzar a la red B, ejecute alguna aplicación de red en un host en la red A mientras que el analizador de protocolos está adjunto a la red B. Pruebe, que el tráfico de la red A no alcanza a la red B.

4.9.5 Mostrando los Resultados

Una vez que las pruebas hayan pasado con éxito y se hayan cumplido los alcances de diseño, el usuario deberá estar conciente de dichos alcances. Usando los resultados de las pruebas, deberás demostrar que el diseño cumple con los alcances establecidos en base a los requerimientos del usuario en cuanto a desempeño, seguridad, capacidad y escalabilidad, y que el diseño está en el umbral de costo y riesgo del usuario. Puede mostrar los resultados de diferentes maneras, incluyendo las que siguen:

- Publique los resultados en un conciso pero comprensivo reporte.
- Agregue los resultados de las pruebas en el documento de diseño de la red.
- Realice alguna presentación con los resultados y realiza una comparativa entre los resultados y los alcances del diseño.

Use el siguiente checklist al verificar el prototipo para la funcionalidad y escalabilidad de la red apropiada. Este checklist contiene consejos de como realizar, pero no son reglas. Las

respuestas correctas con respecto a las preguntas para la salud de la red usualmente es “depende de”. El alcance depende de la topología, la configuración de los enrutadores, las aplicaciones de red, requerimientos de los usuarios, y muchos otros factores.

- Ningún segmento Ethernet se satura (no más del 40% de la utilización de red).
- Los enlaces WAN están saturados (no más del 70% de utilización de red).

- Los tiempos de respuesta son generalmente más bajos que 100 milisegundos (1/10 de segundo).
- Ningún segmento tiene más del 20% de broadcast/multicast.
- Ningún segmento tiene más que un error de CRC por millón de bytes de datos.
- En los segmentos Ethernet, menos del el 0.1 por ciento de tramas resulta en colisión.
- Los enrutadores no están sobre utilizados (en 5 minutos no hay más del 75% de utilización del CPU).
- El número de colas de salida tiradas no excede más de 100 en una hora en el enrutador.
- El número de colas de entrada tiradas no excede más de 50 en una hora en el enrutador.
- El número de errores en el buffer no excede más de 25 en una hora en el enrutador.
- El número de paquetes ignorados no excede más de 10 en una hora en cualquier interfaz del enrutador.

5. Calidad de Servicio (QoS)

El termino QoS se refiere a una amplia colección de tecnologías y técnicas de red. La meta de QoS es proporcionar garantías en la capacidad de red para entregar resultados fiables. Los elementos a considerar para el funcionamiento óptimo de la red desde el punto de vista de QoS incluyen a menudo la disponibilidad (*uptime*), el ancho de banda, el estado de latencia (retraso), el *jitter* y la tasa de error.

QoS implica generalmente la priorización del tráfico de la red. La Calidad de Servicio puede ser definida en términos de la red, en términos del funcionamiento de un enrutador o bridge dado o en términos de alguna aplicación en específico. Un sistema de monitoreo de red debe ser desplegado típicamente como parte de QoS, para asegurarse que la red esta trabajando en el nivel deseado.

QoS es un campo en el cual la investigación y el desarrollo han ido creciendo en el ámbito de las redes. Es esencialmente importante para la nueva generación de aplicaciones de Internet como lo es el video bajo demanda y otros servicios. Algunas tecnologías base para el Internet como Ethernet, no fueron diseñadas para soportar prioridad de tráfico o garantizar niveles de funcionamiento, por la tanto es mucho más difícil implementar soluciones QoS.

Las redes LAN no garantizan la mayoría de los parámetros necesarios para la obtención de QoS, tal y como se definen a continuación:

Disponibilidad. La disponibilidad del servicio se mide como esa fracción de un cierto tiempo total durante el cual se proporciona un servicio MAC. Las operaciones que realice el bridge pueden aumentar o bajar la disponibilidad del servicio. Aumenta evitando en el camino de datos aquellos componentes de la red que estén fallando. Disminuye si falla el bridge, si el bridge deniega el servicio o debido al filtrado de tramas de los bridges.

Pérdida de tramas: MAC no garantiza la entrega de las tramas. Estas pueden no alcanzar a los hosts finales como resultado de:

1. Corrupción de la trama durante la transmisión o recepción a través de la capa física.
2. Que la trama sea descartada por el bridge debido a que no pueda transmitirla en el período máximo determinado, desechándola antes de que ésta supere su período de vida máximo.

a) Los búferes donde se almacenan las mismas estén llenos sin darles tiempo a vaciarse.
b) El tamaño de la unidad de datos de servicio sea mayor que el tamaño máximo soportado por el procedimiento MAC empleado en la LAN.
c) En ocasiones es necesario descartar tramas para mantener otras opciones de QoS.

Reordenación de tramas. No se permite la reordenación de tramas según una prioridad de usuario para una determinada combinación fuente y destino.

Duplicado de tramas. MAC no permite duplicar tramas. Los bridges no introducen el duplicado de tramas de datos de usuario. Las posibilidades de duplicar se reducen al envío a través de distintos caminos entre fuente-destino.

*Retardo de Tránsito***.** MAC introduce retardo dependiendo del tipo de medio utilizado. Su valor se calcula sobre las unidades de datos transmitidas con éxito.

También existe el retardo introducido por un determinado bridge, es el tiempo transcurrido entre la recepción de la trama más el tiempo en acceder al medio por el que va a ser transmitido.

Tiempo de vida de la trama. Es un límite superior al retardo de tránsito. El máximo tiempo de vida de una trama es necesario para asegurar las operaciones correctas de los protocolos de capas superiores. Para asegurar este valor máximo los bridges pueden optar por descartar tramas, asegurando así un retardo máximo en cada bridge.

Tasa de error de trama no detectada. MAC introduce un nivel muy bajo de tasa de error de trama no detectado en las tramas ya transmitidas. Para protegerse ante estos errores se utiliza un secuencia de chequeo de trama (FCS) dependiente del método MAC utilizado. El valor de FCS se recalcula cuando estamos ante distintos métodos.

Tamaño máximo de la unidad de datos de servicio. El tamaño máximo de esta unidad de datos varía con el método MAC utilizado. Hay que tener en cuenta que el valor máximo soportado por dos redes LAN es el más pequeño del soportado independientemente por cada una de ellas.

Prioridad. Un parámetro de QoS permitido e incluido por MAC es la prioridad de usuario. La subcapa MAC mapea las prioridades de usuario solicitadas sobre las prioridades de acceso soportadas por cada una de las métodos individuales MAC utilizados. Una utilidad es la posibilidad de gestionar el retardo de transmisión de una trama en un bridge, asociándole una prioridad de usuario a la misma. Este tipo de retardo comprende: retardo en la cola de almacenamiento hasta que la trama logra situarse en primera línea de transmisión sobre el puerto. Este tipo de retardos se gestionan utilizando prioridad de usuario, y retardo de acceso, para la transmisión de la trama. Se usará prioridad de usuario en aquellas tecnologías que soporten más de una prioridad de acceso. La prioridad va a poder ser asignada por el usuario en base a la dirección destino, el puerto de entrada, el puerto de salida, la prioridad de acceso o por VLAN.

Rendimiento. Una red LAN construida con bridges incrementa significativamente el rendimiento en comparación con cualquier simple red de área local, debido a las características de estos elementos anteriormente citadas, entre ellas porque los bridges pueden localizar el tráfico dentro de las redes LANs a través del filtrado de tramas.

Como se puede ver, para el caso de una Ethernet la prioridad de salida de la trama basada en el campo prioridad de acceso va a ser siempre la mínima (0), independientemente de que la prioridad de usuario sea mayor.

5.1 Capa 2

5.1.1 Conmutación

Una red conmutada de datos consiste en una sucesión alternante de nodos y canales de comunicación, es decir, después de ser transmitida la información a través de un canal, llega a otro nodo, éste a su vez, la procesa lo necesario para poder transmitirla por el siguiente canal para llegar al siguiente nodo, y así sucesivamente.

Existen dos tipos de conmutación en este tipo de redes: conmutación de paquetes y conmutación de circuitos.

5.1.1.1 Conmutación de circuitos (*Circuit Switching*)

La conmutación de circuitos es un tipo de comunicación que establece o crea un canal dedicado (o circuito) durante la duración de una sesión. Después de que es terminada la sesión (por ejemplo: una llamada telefónica) se libera el canal y éste podrá ser usado por otro par de usuarios.

El ejemplo más típico de este tipo de redes es el sistema telefónico la cual enlaza segmentos de cable para crear un circuito o trayectoria única durante la duración de una llamada o sesión. Los sistemas de conmutación de circuitos son ideales para comunicaciones que requieren que los datos sean transmitidos en tiempo real.

Existen dos variantes en la conmutación de circuitos:

Multicanalización por División de Tiempo (*TDM: Time Division Multiplexing* Un multicanalizador basado en TDM empaqueta un conjunto de información (tramas de bits) de diferentes fuentes en un solo canal de comunicación en tiempos (muy cortos) diferentes. En el otro extremo estas tramas son otra vez reensambladas y llevadas a su respectivo canal. Los mux TDM como manejan tramas de bits son capaces además de comprimir la información al eliminar redundancias en los paquetes, muy útil en el caso de aplicaciones de voz. La información analógica es primero convertida a formato digital antes de la transmisión.

Multicanalización por División de Frecuencias (*FDM: Frequency Division Multiplexing*): Los multicanalizadores en FDM tienen como entrada varios canales trabajando en diferentes frecuencias y las combina en un solo ancho de banda. En televisión por cable, la red de cable es usada para contener diferentes canales de televisión los cuales utilizan diferentes frecuencias y cuyo ancho de banda de cada canal es de 6MHz. Un espectro típico de este tipo de sistemas es de 500 a 800MHz de ancho de banda, el cual es suficiente para dar cabida a más de 80 canales de programación. Cada canal funciona separadamente, los cuales al ser sintonizados en el televisor se desmulticanaliza un canal a la vez.

5.1.1.2 Conmutación de paquetes (*Packet Switching*)

En los sistemas basados en conmutación de paquetes, los datos a ser transmitida previamente es ensamblada en paquetes. Cada paquete es entonces transmitido individualmente y éste puede seguir diferentes rutas hacia su destino. Una vez que los paquetes llegan a su destino, los paquetes son otra vez reensamblados

Mientras que la conmutación de circuitos asigna un canal único para cada sesión, en los sistemas de conmutación de paquetes el canal es compartido por muchos usuarios simultáneamente. La mayoría de los protocolos de WAN tales como TCP/IP, X.25, Frame Relay, ATM, son basados en conmutación de paquetes.

La conmutación de paquetes es más eficiente y robusta para datos que pueden ser enviados con retardo en la transmisión (no en tiempo real), tales como el correo electrónico, paginas Web, transmisión de archivos, etc.

En el caso de aplicaciones como voz, video o audio la conmutación de paquetes no es muy recomendable a menos que se garantice un ancho de banda adecuado para enviar la información. Pero el canal que se establece no garantiza esto, debido a que puede existir tráfico y nodos caídos durante el recorrido de los paquetes. Estos son factores que ocasionen que los paquetes tomen rutas distintas para llegar a su destino. Por eso se dice que la ruta que toman los paquetes es probabilística, mientras que en la conmutación de circuitos, esta ruta es determinística.

Hay dos técnicas básicas para el envío de estos paquetes:

1. *Técnica de datagramas:* cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control (Por ejemplo número de paquete, nombre, dirección de destino, etc.) y lo envía hacia su destino. Puede ocurrir que por haber tomado caminos diferentes, un paquete con número por ejemplo 6 llegue a su destino antes que el número 5. También puede ocurrir que se pierda el paquete número 4. Todo esto no lo sabe ni puede controlar el emisor , por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido (para su posible reclamación al emisor), y para esto, debe tener el software necesario.
2. *Técnica de circuitos virtuales:* antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de Petición de Llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes. Este camino virtual será numerado o nombrado inicialmente en el emisor y será el paquete inicial de Petición de Llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número. De esta forma, el encaminamiento sólo se hace una vez (para la Petición de Llamada) . El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez.

La conmutación es una tecnología que reduce la congestión en las LAN Ethernet, Token Ring y la Interfaz de Datos Distribuida por Fibra (FDDI) reduciendo el tráfico y aumentando el ancho de banda. Los switches se utilizan frecuentemente para reemplazar los concentradores compartidos. Están diseñados para funcionar con infraestructuras de

cable ya existentes, de manera que se puede instalar sin provocar disturbios en el tráfico de red existente. Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas:

a) Conmutación de tramas de datos: Esto ocurre cuando una trama llega a un medio de entrada y se transmite a un medio de salida.
b) Mantenimiento de las operaciones de conmutación: un switch desarrolla y mantiene las tablas de conmutación.

El término bridging se refiere a la tecnología en la cual un dispositivo (puente) conecta dos o más segmentos de la LAN. Un bridge transmite tramas de un segmento a otros. Cuando un bridge se activa y empieza a operar, examina la dirección MAC de los tramas entrantes y crea una tabla de destinos conocidos. Si el destino de una trama se encuentra en el mismo segmento que el origen la trama se descarta. Si el destino se encuentra en otro segmento se transmite a ese segmento. Si no se conoce el destino, se transmite a todos los segmentos salvo el origen (inundación). El bridging limita el tráfico.

Los bridges y switches conectan segmentos LAN, utilizan una tabla de direcciones MAC para saber el segmento al destino y reducen tráfico. Los switches son más funcionales que los bridges en las redes actuales porque operan a una velocidad mucho más alta que los bridges y soportan nuevas funcionalidades, como por ejemplo las VLANs. Los bridges se conectan generalmente utilizando software; los switches se conectan generalmente utilizando hardware.

La conmutación empleada en un switch es la *cut-through*, el la cual el switch una vez que ve la dirección MAC del destinatario la empieza a transmitir aunque no le haya llegado la trama completa todavía. Los switches de capa 2 utilizan la microsegmentación para satisfacer las necesidades de ancho de banda. La conmutación permite que muchos usuarios se comuniquen en paralelo a través de los circuitos virtuales del switch. Esto permite maximizar el ancho de banda de la red.

Se puede asignar dos tipos de conmutación a los puertos del switch:

Conmutación Simétrica: Este tipo de conmutación se caracteriza por la asignación de un ancho de banda a cada puerto. Todos los puertos tienen el mismo ancho de banda.

Conmutación Asimétrica: Este tipo de conmutación asigna un ancho de banda diferente a cada puerto dependiendo de sus necesidades en cada momento determinado.

La diferencia entre la conmutación de capa 2 y capa 3 es el tipo de información que se encuentra dentro de la trama y que se utiliza para determinar la interfaz de salida correcta. Con la conmutación de capa 2, las tramas se conmutan tomando como base la información de la dirección MAC. Con la conmutación de capa 3, las tramas se conmutan tomando como base la información de la capa de red.

5.1.2 Clase de Servicio (CoS)

La clase del servicio es una manera de manejar tráfico en una red agrupando tipos de tráfico similares (por ejemplo, e-mail, vídeo en línea, voz, transferencia de archivos de gran tamaño) juntos y tratando cada tipo como una clase con su propio nivel de prioridad

de servicio. Al contrario de lo que ofrecen la administración basada en QoS, las tecnologías de CoS no garantizan un nivel en lo que se refiere al ancho de banda y al tiempo de entrega de la información; ofrecen el concepto de mejor-esfuerzo. Por otra parte, la tecnología CoS es más simple de manejar y más escalable a medida que una red crece en volumen y en tráfico.

Para CoS los parámetros de calidad son especificados en el switch o en el enrutador: el equipo es preconfigurado para asignar recursos y dar tratamiento especial a ciertas clases de tráfico, los recursos son asignados a una parte del tráfico de la red, no hay necesidad de señalización puesto que la asignación no es echa en base a flujos, el equipo de comunicaciones supone que los recursos no serán sobre-extendidos y que el tráfico que llegue sea de manera controlada, el equipo no hace nada por asegurarse de lo anterior.

CoS crea categorías de tipos de tráfico. Puede verse como un método para diferenciar el tráfico y aplicarle un tratamiento especial, todo el tráfico en el interior de cierta CoS es tratado de manera similar que otro tráfico dentro de la misma categoría. Además puede haber parámetros específicos de calidad para cada CoS: no necesita mantener una gran cantidad de información y cada paquete es tratado de manera independiente.

De manera práctica, si el tráfico de cierto CoS supera determinado umbral, este tiene que tomar recursos de otro CoS o bien el tráfico no recibe más la calidad requerida. Hay tres maneras de hacer ingeniería de red para evitar estos problemas de sobre-suscripción: Sobre-ingeniería, Protocolos de Señalización y Servidor de Políticas

5.1.3 802.1p

Lo norma IEEE 802.1p es un mecanismo de control para Prioritización del tráfico en capa 2, para el uso redes LAN. Define un campo en el encabezado de acceso al medio (MAC) de los paquetes Ethernet, que puede transportar uno de los ocho valores preferentes. Los hosts o los enrutadores que envían tráfico a una LAN marcan cada paquete transmitido con el valor de preferencia adecuado. Los dispositivos LAN, tales como bridges o concentradores deben tratar los paquetes de forma adecuada. El ámbito de la prioridad de usuario 802.1p está limitado a la LAN. También ofrece filtrado de tráfico multicast para asegurar que este no prolifere sobre las redes que utilizan switches en capa 2.

La propuesta de la IEEE 802.1p es una extensión de la norma 802.1D que dicta como debe hacerse la prioritización en la capa MAC de un bridge independientemente del medio. Por otro lado, el 802.1Q, la norma para VLANs, añade prioritización a los servicios Ethernet en particular. Con el uso de equipo con características 802.1p/Q es posible implementar servicios de prioritización completos. La funcionalidad 802.1p se logra a través del uso de 3 bits para prioridad de usuario independientemente de la topología utilizada. Las tramas entrantes pueden ser examinadas buscando un valor de prioridad preexistente, que es mapeado al valor específico del 802.1p. Este valor puede ser asignado a una trama saliente u otro medio. Sin embargo, Ethernet nunca había tenido el servicio de prioritización de forma nativa, por lo que la propuesta 802.1Q complementa perfectamente esta carencia. La implementación de la 802.1Q se hace con cuatro bytes adicionales insertados en el encabezado de la trama. Estos 4 bytes contienen una variedad de campos, la mayoría de los cuales son específicos de a los datos de la VLAN, pero uno de ellos provee una bandera de 3 bits. Estos 3 bits proveen 8 valores posibles, los mimos usados en el esquema de mapeo de prioridad del 802.1p. En redes Ethernet,

los campos del encabezado 802.1Q son insertados en las tramas inmediatamente después de los campos de direcciones fuente y destino, y antes del campo de longitud. Con la supremacía a últimas fechas de las redes Ethernet, Fast Ethernet y Gigabit Ethernet; y el advenimiento de nuevas y complejas aplicaciones en línea, es casi imprescindible que el equipo seleccionado para la red local cuente con estas características para poder tener un mejor control del ancho de banda.

La norma 802.1p permite 8 tipos de clases de tráfico clasificados como prioridades de usuario por cada puerto del bridge, siendo el rango de valores de prioridad de usuario del 0 al 7.

A continuación, en la Figura 1, se muestra el Frame Ethernet Etiquetado con la norma 802.1Q:

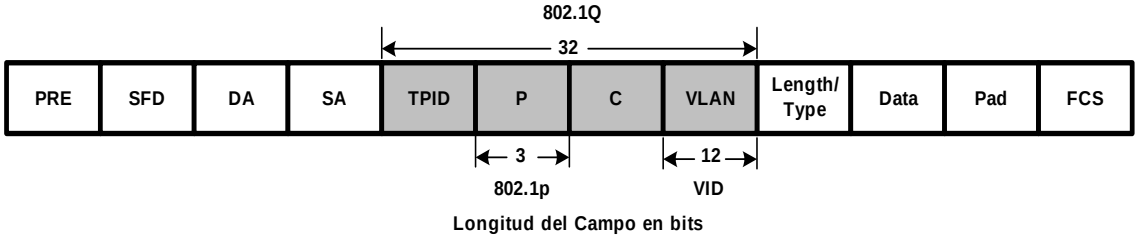


Figura 1. Trama Ethernet etiquetada con la norma 802.1Q

Donde,

TPID: Este campo (12 bits) es un valor hexadecimal definido en 8100. Cuando una trama tiene este valor, se entiende que esta etiquetado con la norma IEEE 802.1Q/802.1p.

P: Define la prioridad de usuario, dada por 8 niveles de prioridad, la norma IEEE 802.1p define la operación para estos 3 bits.

C: Es un indicador que siempre esta en 0 para los switches Ethernet, este campo es utilizado por razones de compatibilidad entre redes del tipo Ethernet y Token Ring. Si una trama que llega a un puerto Ethernet tiene este campo con valor 1, esta trama no será enviada a un puerto no etiquetado.

VLAN: Este campo es un identificador de VLAN, el cual es básicamente usado por la norma IEEE 802.1Q. Es de 12 bits y permite identificar 4096 (2^{12}) VLANs, de estos 4096 ID posibles; el valor 0 es usado para identificar tramas con prioridad y el valor de 4095 (FFF) es reservado, entonces el valor máximo de VLANs posible es de 4094.

En la siguiente tabla se pueden observar las prioridades:

Prioridad de usuario	Prioridad de usuario por defecto	Rango
0	0	0-7
1	1	0-7
2	2	0-7
3	3	0-7
4	4	0-7
5	5	0-7
6	6	0-7
7	7	0-7

Tabla 2. Tabla de Prioridades

La prioridad del tráfico en redes LAN va a depender también del número de colas existentes en cada puerto. El almacenamiento de las tramas en estas colas se realiza en base al campo prioridad de usuario y a la dirección origen y destino para el tráfico Unicast y en base al campo prioridad de usuario y la dirección destino para tramas Multicast.

Una vez determinadas las clases de tráfico por bridge, será necesario mapearlas (asociarlas) con el tipo de tráfico que circule por la red para asegurar que el tráfico en tiempo real (por ejemplo) sea atendido antes que el tráfico para el que un servicio de mejor esfuerzo es más que suficiente. La siguiente tabla muestra cómo se podría asociar el campo prioridad de usuario al tipo tráfico y sus características:

Prioridad de usuario	Tipo de tráfico	Características del trafico
0	Mejor Esfuerzo (*Best Effort*)	Tráfico de red como lo conocemos ahora.
1	Diferida (*Background*)	Actividades y transferencia de información que no impactan en el rendimiento de la red y a los usuarios.
2	*Spare*	Valor de Repuesto.
3	Esfuerzo Excelente (*Excellent Effort or Business Critical*)	Este tipo de servicios contienen información de la organización que debe ser entregada a los clientes más importantes.
4	Aplicaciones de carga controlada (*Controlled Load*)	Aplicaciones importantes para negocios de admisión controlada, planeadas para reservar ancho de banda de un extremo a otro.
5	Vídeo interactivo	Caracterizado por menos de 100ms de retraso.
6	Voz interactiva	Caracterizado por menos de 10ms de retraso.
7	Control de red (*Network Control*)	Requerida para mantener y soportar la infraestructura de red, caracterizada por su gran importancia.

Tabla 3. Asociación de la prioridad de usuario

5.2 Capa 3

5.2.1 Prioridad IP y TOS

El campo Tipo de Servicio ocupa un octeto de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, y 7 esta reservado para control de red. Muchos gateways ignoran este campo.

Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el coste monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los enrutadores para direccionar las solicitudes de los usuarios.

El datagrama que hace referencia al Tipo de Servicio y a los Servicios Diferenciados, es el campo Tipo de Servicio que especifica como el datagrama debe ser dirigido o enviado. El campo se divide en cinco subcampos como se muestra en la Figura 2.

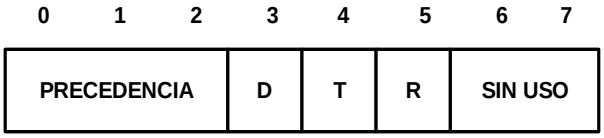


Figura 2. Los cinco subcampos que conforman el campo tipo de servicio de 8 bits.

Los tres primeros bits especifican la precedencia del datagrama, con valores entre el rango de 0, para precendencia normal, hasta 7, para control de red. Este subcampo permite a los emisores indicar la importancia en el envío de cada datagrama. A pesar de que algunos enrutadores ignoran el concepto de Tipo de Servicio, este es un concepto importante ya que provee un mecanismo que permite controlar la información para tener precendencia en los datos. Por ejemplo, algunos enrutadores usan un valor de precedencia de 6 o 7 para el tráfico de enrutamiento para hacer posible que los enrutadores intercambien información de enrutamiento aún cuando la red este congestionada.

Los bits D, T y R especifican el tipo de transporte deseado para el datagrama, Cuando estos bits son encendidos, el bit D especifica bajo retraso, el bit T especifica un alto rendimiento en el procesamiento, y el bit R una alta confiabilidad. Claro, no puede ser posible para una red garantizar el tipo de transporte deseado (por ejemplo, puede ser que ningún camino hacia el destino tenga la característica requerida). Esto es, el transporte requerido para la transmisión de datos no tiene relación alguna con los algoritmos de enrutamiento, no como una demanda. Si un enrutador conoce más de una posible ruta para un destino dado, este puede usar el campo de tipo de transporte para seleccionar uno con las características más cercanas al deseado. Por ejemplo, si se supone que un enrutador puede seleccionar entre una línea de baja capacidad y una conexión satelital con gran ancho de banda, pero con gran lentitud. Los datagramas que contienen información desde un usuario hacia un host remoto pueden tener el bit D encendido,

requiriendo que estos sean entregados lo más rápido posible, mientras que los datagramas que contienen una gran transferencia de archivos pueden tener el bit T encendido requiriendo que ellos viajen a través de un enlace satelital de alta capacidad.

5.2.2 Calidad de Servicio IP a través de DiffServ

A finales de los años 90s, la IETF redefinió el significado del campo Tipo de Servicio para acomodarlo como un arreglo de Servicios Diferenciados. La Figura 3 ilustra la definición resultante.

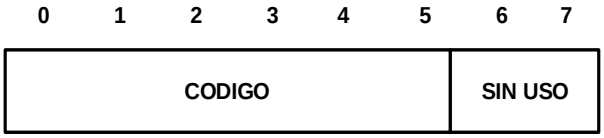


Figura 3. La Interpretación de los Servicios Diferenciados (DS) del campo de Tipo de Servicio en un datagrama IP

DiffServ define un conjunto de tipos de servicios y mecanismos QoS aplicados a paquetes en esos tipos de servicios (llamados Comportamientos Per-Hop o PHBs). El Punto de Código de DiffServ (DSCP) está ubicado en el cabezal del paquete IP y es usado para determinar el PHB. Cada norma PHBs tiene un único DSCP asociado. El DSCP es utilizado para determinar el comportamiento de DiffServ respectivo, que el paquete va a recibir. Diferentes tipos de aplicaciones tienen diferentes características de tráfico y requieren distintos tipos de comportamientos de QoS.

Bajo la interpretación de los Servicios Diferenciados, los primeros 6 bits abarcan un código, el cual a veces es abreviado como DSCP, y los últimos 2 bits aún no tienen uso. Un valor en el código de 6 bits mapea hacia una definición de servicios subyacentes, típicamente a través de un arreglo de punteros. Aunque es posible definir 64 servicios separados, los diseñadores sugieren que un enrutador dado solo tendrá pocos servicios, y códigos múltiples mapearán hacia cada servicio. Más aún, para mantener compatibilidad reciproca con la definición original, la norma distingue entre los 3 primeros bits del código (los bits que formalmente fueron usados para la precedencia) y los tres últimos bits. Cuando los tres últimos bits tiene valor 0, los bits de precedencia definen ocho amplias clases de servicio que se adhieren a los mismos lineamientos de la definición original: los datagramas con un valor mayor en su campo de precedencia se les da un trato preferencial sobre los datagramas con un valor menor. Esto es, las ocho clases ordenadas son definidas por los valores del código de la forma siguiente:

xxx000

Donde x denota tanto a un cero como a un uno.

El diseño de los Servicios Diferenciados también comprende otra práctica existente: el extenso uso de la precedencia 6 o 7 para el tráfico de enrutamiento. La norma incluye un caso especial para estos valores de precedencia. Un enrutador requiere implementar al menos dos esquemas de prioridad: uno para el tráfico normal y otra para el tráfico de alta

prioridad. Cuando los últimos 3 bits del código están en 0, el enrutador debe mapear un código con precedencia 6 o 7 en la clase de más alta prioridad y otro valor de código en la clase de más baja prioridad. Esto es, si un datagrama arriva y este fue enviado usando el esquema original de Tipo de Servicio, un enrutador usando el esquema de Servicios Diferenciados honrará a la precendencia 6 o 7 como la expectativa de datagramas enviados.

Los 64 valores del código son divididos en tres grupos administrativos, como se ilustra en la Figura 4.

GRUPO	CODIGO	ASIGNADO POR
1	**xxxxx0**	**Organización Normativa**
2	**xxxx11**	**Local o Experimental**
3	**xxxx01**	**Local o Experimental por ahora**

Figura 4. Los tres grupos administrativos de valores de código

Como la figura lo indica, la interpretación de la mitad de los valores (por ejemplo, los 32 valores en el grupo 1) deben estar asignados por la IETF. Actualmente, todos los valores en los grupos 2 y 3 están disponibles para uso experimental o local. Sin embargo, si las normas terminan por ocupar todos lo valores en el grupo 1, se puede escoger la asignación de valores en el grupo 3.

La división en grupos puede verse inusual por que esta confía en los bits de orden menor del valor para distinguir entre grupos. Esto quiere decir, más que un arreglo contiguo de valores, el grupo 1 contiene todos los demás valores de código (por ejemplo, todos lo números entre 2 y 64). La división fue escogida para mantener los 8 códigos correspondientes para los valores xxx000 en el mismo grupo.

Si la interpretación original de Tipo de Servicio o la revisada interpretación de Servicios Diferenciados es usada, es importante analizar que el software de enrutamiento debe escogerse desde un gran conjunto de bien delineadas topologías físicas de red por un lado y debe ser complemento de la red ya establecida. Por lo tanto, especificar un nivel de servicio en el datagrama no garantiza que los enrutadores respetarán lo requerido a lo largo de todo el enlace.

En resumen: Se mira la especificación del Tipo de Servicio como indirecta hacia los algoritmos de enrutamiento y esta ayuda a los mismos a escoger entre varios caminos hacia el destino basándose en políticas locales de red y en su conocimiento de las tecnologías de hardware disponibles en esos enlaces. Una red no garantiza proporcionar un particular tipo de servicio.

El Punto de Código del DiffServ localizado en el encabezado del paquete IP se usa para determinar el PHB, ocupa el campo del Tipo de Servicio (ToS), pero no es compatible con éste.

Cada PHB tiene un único DSCP asociado que determina el comportamiento de DiffServ que recibirá el paquete. Distintos tipos de aplicaciones poseen distintas características de tráfico y, por lo tanto, requieren distintos tipos de comportamiento de QoS. Asimismo, los

PHBs de hábito también se pueden crear usando su DSCP único para identificarlos. Se tienen los siguientes DSCPs:

Envío Expedito (Expedited Forwarding DiffServ Class): El comportamiento DiffServ de Envío Expedito (EF) brinda un servicio de alta prioridad y baja latencia, ideal para VoIP. Se implementa con una alta prioridad de emisión (o la más alta) y la prioridad de descarte más baja. Para obtener el comportamiento deseado, cada nodo de la red debe asegurar que el tráfico EF tenga los niveles más bajos posibles de delay, jitter y pérdida, ya que el servicio intentará emular una línea rentada sobre la red IP.

Envío Asegurado (Assured Forwarding DiffServ Class): El comportamiento DiffServ de Envío Asegurado (AF) consiste en cuatro tipos de servicios diferentes, cada uno con tres niveles de prioridad de descarte. La Clase 4 tiene una prioridad de emisión más alta que la Clase 3. La Clase 3 tiene una prioridad de emisión más alta que la 2, y así sucesivamente. Cuanto más grande sea el número, más alta será la prioridad de emisión. Cada clase de AF tiene tres clases de prioridad de descarte, también llamadas niveles de precedencia de caída. Esto da como resultado 12 valores DSCP. Los enrutadores usan estos valores de precedencia de caída para determinar la prioridad de descarte de los paquetes en caso de congestión en la red.

Selector de Clase (Class Selector DiffServ): El comportamiento DiffServ de Selector de Clase (CS) se representa por ocho clases de prioridades que utilizan las mismas posiciones de bits que el campo de precedencia IP en la definición de ToS. El DSCP CS7 tiene la prioridad de envío más alta y el DSCP CS0 tiene la prioridad de envío más baja. El CS0 equivale al servicio de esfuerzo mayor. El comportamiento CS no soporta prioridades de descarte.

DiffServ de Omisión (Default DiffServ class): El comportamiento de Omisión (DE) se usa para transportar el tráfico de mayor esfuerzo. Cualquier otro tipo de tráfico que no sea clasificado bajo otra norma o hábito debe ser transportado usando PHB DE. El valor del DSCP DE es 0 y, en general, tiene la prioridad de descarte más alta y la de emisión más baja.

5.2.2.1 Mapeo de DiffServ en capa 3

DiffServ brinda un conjunto de clases de servicio estándar que se denominan PHBs (Per Hop Behavior). Las PHBs también brindan un valor de Punto de Código DiffServ normalizado asociado con el PHB. Por eso, el DSCP debe mapearse de acuerdo a las distintas capas de enlace QoS, para brindar el comportamiento más cercano posible al deseado y crear un servicio de punta a punta.

Hay muchas posibilidades en cuanto a cómo mapear la Calidad de Servicio IP, de acuerdo a la Calidad de Servicio de las capas de enlace. A continuación, se presenta un modelo de mapeo de capa de enlace que puede ser utilizado para brindar un comportamiento consistente entre el IP y las tecnologías QoS de las capas de enlace.

Ethernet brinda ocho clases de servicios a través de los tres bits 802.1p. Estas ocho clases se usaron tradicionalmente para brindar ocho niveles de prioridad. DiffServ puede

ser mapeado de acuerdo a las prioridades del usuario de Ethernet 802.1p, como se muestra en la siguiente tabla:

Punto de Código de DiffServ (DSCP)	Prioridad de usuario de Ethernet 802.1p
CS7, CS6	7
EF, CS5	6
AF4x1, CS4	5
AF3x1, CS3	4
AF2x1, CS2	3
AF1x1, CS1	2
DE, CS0	0

1x = 1, 2 o 3

Tabla 3. Ocho clases, ocho niveles de prioridad

En este ejemplo no se utiliza la prioridad 1 de los usuarios de 802.1p. La prioridad 0 de los usuarios de 802.1p debe ser el valor por omisión para el tráfico de mayor esfuerzo, que es la razón por la cual está mapeado de acuerdo al DE (default) del PHB del DiffServ.

5.2.3 Servicios Integrados IntServ y Protocolo RSVP

En la arquitectura IntServ ocupa un papel fundamental el concepto de flujo. Se entiende por flujo un tráfico continuo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requiere una misma Calidad de Servicio. Un flujo es unidireccional y es la entidad más pequeña a la que puede aplicarse una determinada Calidad de Servicio. Los flujos pueden agruparse en clases; todos los flujos de una misma clase reciben la misma calidad de servicio.

En IPv4 los flujos se identifican por las direcciones de origen y destino, el puerto de origen y destino (a nivel de transporte) y el protocolo de transporte utilizado (TCP o UDP). En IPv6 la identificación puede hacerse de la misma forma que en IPv4, o alternativamente por las direcciones de origen y destino y el valor del campo Etiqueta de Flujo. Aunque el campo Etiqueta de Flujo en IPv6 se definió con este objetivo la funcionalidad aún no se ha implementado en la práctica.

En la arquitectura IntServ se definen tres tipos de servicio:

- *Servicio Garantizado:* garantiza un caudal mínimo y un retardo máximo. Cada enrutador de la ruta debe ofrecer las garantías solicitadas, aunque a veces esto no es posible por las características del medio físico (por ejemplo en Ethernet compartida).
- *Servicio de Carga Controlada:* este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada, es decir en general un buen tiempo de

respuesta, pero sin garantías estrictas. Eventualmente se pueden producir retardos grandes.

- *Servicio Best Effort:* este servicio no tiene ninguna garantía.

Para conseguir sus objetivos IntServ dispone del protocolo RSVP. El protocolo RSVP (*Resorce reSerVation Protocol*) está pensado fundamentalmente para tráfico multicast, ya que este tipo de tráfico es especialmente adecuado para la distribución de flujos de audio y vídeo en tiempo real que requieren unas condiciones estrictas de calidad de servicio. Sin embargo nada impide la utilización de RSVP en tráfico unicast.

En una emisión multicast los usuarios pueden apuntarse o borrarse del grupo multicast de forma dinámica y sin advertencia previa; por ejemplo, una red emite de forma multicast diversos programas simultáneamente (equivalente a canales de televisión) y que los usuarios desde sus hosts van continuamente haciendo *zapping* de un canal a otro; en un momento dado los usuarios que estén viendo un determinado canal forman un grupo multicast, pero el grupo puede cambiar con rapidez. Suponiendo que todos los programas se emiten desde el mismo host, este host será la raíz del árbol de expansión (*spanning tree*) de la emisión multicast; para cada programa multicast que se emite hay un conjunto de receptores que configuran un árbol de expansión diferente; esto es tarea del protocolo de enrutamiento multicast, no de RSVP. Por tanto a partir de aquí se supone resuelta esa parte del problema.

El primero de los receptores del programa provoca la creación por parte del protocolo de enrutamiento del árbol de expansión y envía un mensaje de reserva hacia el emisor empleando el enrutamiento del camino inverso que se ha visto al hablar de enrutamiento multicast. Cada enrutador por el que pasa el mensaje de reserva toma nota del ancho de banda solicitado y lo reserva, o bien devuelve un mensaje de error si no hay capacidad disponible. Si todo va bien al final del proceso el receptor ha reservado el ancho de banda necesario en todo el camino hasta la raíz del árbol.

Cuando aparece en la red un segundo receptor de esa misma emisión multicast envía su mensaje de reserva, pero la reserva sólo se efectuará en aquella parte de la ruta (o rama del árbol) que no sea común con el primer receptor y no haya sido por tanto ya reservada por éste. De esta forma se asegura un uso óptimo de la red, no reservando caudal dos veces en el mismo enlace, a la vez que se evita por completo la congestión.

Es evidente, que aunque se trate de un protocolo Internet RSVP es un protocolo orientado a conexión, ya que los enrutadores tienen que guardar una cierta información de estado de cada flujo para el que se efectúa reserva, algo equivalente a un circuito virtual. Se dice entonces que los Enrutadores con RSVP ya no son *stateless* sino *statefull*.

5.2.4 Técnicas de encolamiento

Las técnicas de encolamiento se basan en la programación de paquetes y contribuyen a tener una mayor eficiencia y bajar el costo del Ancho de Banda en una red basada en paquetes. Además de controlar la velocidad a la cual los usuarios ganan acceso al Ancho

de Banda, también asegura que aquel que esta transmitiendo dentro de lo especificado, no se verá afectado por quien no lo esta haciendo.

Los esquemas de programación de salida son:

- FIFO (*First in, First Out*)
- PQ (*Priority Queuing*)
- CQ (*Custom Queuing*)
- CBQ (*Class Based Queuing*)
- WFQ (*Weighted Fair Queuing*)
- WFQ/RED (*Weighted Fair Queuing with Random Early Discard*)

5.2.4.1 FIFO: Primero en Entrar Primero en Salir (*First in, First Out*)

Es un método estricto de encolamiento para la transmisión de paquetes en el orden en que son recibidos, el primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por omisión en las redes IP. Es válido solo en redes con mínima congestión. No provee protección, no analiza el ancho de banda ni la posición en la cola de espera.

5.2.4.2 PQ: Encolado con Prioridad (*Priority Queuing*)

Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles que puede aportar el encabezado del datagrama IP (ToS). Se trata de 3 bits disponibles en el Byte 2 del encabezado de IPv4 (bits de precedencia).

Aquí los paquetes son expuestos en el espacio del buffer de acuerdo a su nivel de prioridad, los paquetes con mayor prioridad son enviados al enlace de salida antes que los paquetes con baja prioridad. El problema existente en este tipo de encolamiento es que puede retrasar demasiado el tráfico de baja prioridad volviéndolo inútil.

5.2.4.3 CQ: Encolado Aleatorio (*Custom Queuing*)

Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. El operador reserva un espacio de búfer y una asignación temporal a cada tipo de servicio. Es una reservación estática.

5.2.4.4 CQB: Encolado en Base a Clase (*Class Based Queuing*)

Es un método de encolamiento en el cual el tráfico es divido en clases y separado en colas de acuerdo al tipo de clase asignada, este tipo de encolamiento asigna el espacio del buffer de acuerdo a su prioridad, de manera que implementa un esquema más equitativo. El usuario configura la preferencia con la cual la cola será servida y la cantidad de tráfico liberado al enlace en cada pase.

La limitante es que la asignación del buffer es estática, por lo que debe de configurar suficiente capacidad para acomodar todas las clases de tráfico. Se vuelve necesaria la administración del búfer ya que el algoritmo de programación no puede por si solo asegurar una asignación equitativa.

Idealmente, todo el espacio del búfer debe estar disponible para todo tipo de tráfico: realizado de tal manera que el tráfico de precedencia más alta no sea privado de este espacio por paquetes de menor precedencia o no conformes; esta es la principal razón por la cual se necesita un esquema inteligente de descarte.

5.2.4.5 WFQ: Encolamiento Equitativo Ponderado (*Weighted Fair Queuing*)

Este método permite múltiples colas definidas para variados flujos de tráfico. El administrador crea diferentes tamaños de cola y delega que tipo de tráfico es destinado para cada cola en particular, este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket–Port* de TCP/UDP-) y por el ToS en el protocolo IP. En este esquema la menor ponderación es servida primero. Con igual ponderación es transferido con prioridad el servicio de menor ancho de banda. El protocolo de reservación RSVP utiliza a WFQ para localizar espacios de buffer y garantizar el ancho de banda.

5.2.4.6 WQF/RED: Encolamiento Equitativo Ponderado con Descarte de Paquetes Voluntario (*Weighted Fair Queuing con Random Early Discard*)

Esta es una técnica de encolamiento para manejar inteligentemente el espacio en el búfer, se basa en la influencia sobre el tipo de tráfico que es permitido entrar a la red y provee de asignaciones de Ancho de Banda y limites de retardo para tipos específicos de tráfico.

En esta técnica no es necesaria la intervención del usuario para asignar el espacio en búfer, además usa un algoritmo de servicio que intenta proveer retardos predecibles. Según llegan los paquetes, el búfer es ordenado de tal manera que intenta asegurar que cada paquete sea retrasado la cantidad de tiempo apropiado. WFQ reenvía los paquetes justo antes de que se alcance el máximo retardo para esa prioridad y mejora los tiempos de respuesta reduciendo las variaciones de retardo en el tráfico interactivo resultando en retardos más predecibles.

WFQ necesita de un mecanismo de control para el tráfico que entra a la red, por lo tanto cuando ocurre congestión, el proveer retardos más apropiados se hace más complicado y RED comienza a tirar paquetes selectivamente forzando a las sesiones de TCP a disminuir el tráfico. Desafortunadamente es un método reactivo.

6. Resolución de Problemas

Las fallas en la interconectividad entre redes se caracterizan por ciertos síntomas. Pueden ser generales o específicos: desde clientes que no pueden tener acceso a determinados servidores hasta rutas que no están incluidas en la tabla de enrutamiento. Cada síntoma debe ser analizado utilizando herramientas y técnicas específicas para la solución de problemas. Una vez identificado el problema o la causa de este se puede remediar implementando una solución consistente en una serie de acciones.

6.1 Modelo General para la resolución de problemas

La mejor opción para resolver problemas en un entorno de red es emplear un enfoque sistemático. Se debe definir los síntomas específicos y los problemas potenciales, posteriormente eliminar cada problema potencial de manera sistemática hasta que desaparezcan los síntomas.

La Figura 1, ilustra el flujo de procesos del modelo general de resolución de problemas. Este no es un esquema rígido, sin embargo, constituye la base para generar un proceso de resolución que satisfaga a un entorno en particular.

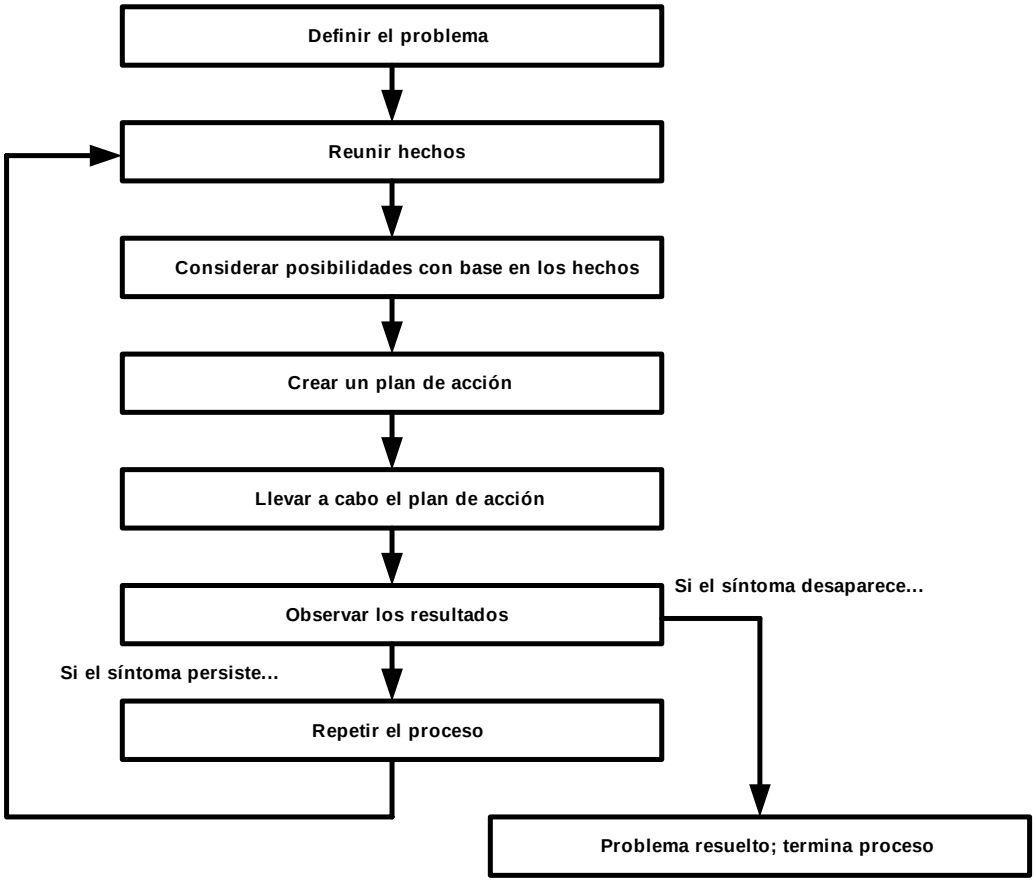


Figura 1. Modelo general de resolución de problemas

Los siguientes pasos detallan este proceso:

1. Al analizar un problema de red, construir un enunciado claro del problema. Definiendo el problema en términos de un conjunto de síntomas y causas potenciales.
2. Reunir los hechos que necesita para aislar las posibles causas.
3. Considerar los posibles problemas con base en los hechos reunidos. Mediante el uso de estos eliminar de la lista algunos de los problemas potenciales.
4. Crear un plan de acción basado en los problemas potenciales restantes, comenzando por el más probable, concibiendo un plan en el que solo se manipule una variable a la vez.
5. Poner en marcha el plan de acción, realizando con cuidado cada paso al tiempo que comprueba si desaparece el síntoma.
6. Siempre que se cambie una variable, asegurar la recopilación de los resultados.
7. Analizar los resultados para determinar si se resolvió el problema. De ser así, entonces el proceso esta concluido.
8. Si el problema no se resolvió, se debe crear un plan de acción basado en el siguiente posible problema de la lista. Regresar al paso 4, cambiar una variable a la vez y repetir el proceso hasta que se resuelva el problema.

6.2 Prevención de fallas en la red

Siempre será más fácil recuperarse de una falla de red si se esta prevenido. Posiblemente el requerimiento más importante en cualquier entorno de red sea tener disponible en todo momento, para el personal de soporte de la misma, la información actual y precisa a cerca de la red. Sólo con información completa se pueden tomar decisiones inteligentes acerca de un cambio en la red, y sólo con la información completa puede efectuarse la resolución de problemas en la forma más rápida y sencilla posible. Durante el proceso de resolución de problemas de la red, es aspecto más critico por asegurar es que esta información se mantenga actualizada.

Para prevenir una falla de red se debe contar con lo siguiente:

- *Mapa físico y lógico preciso de la red:* Ubicación física de todos los dispositivos en la red y como están conectados, mapa lógico de las direcciones de red, los números de red, las subredes, etc.
- *Protocolos implementados en la red:* Lista de los números de red, subredes, zonas, áreas y demás, asociados a dichos protocolos.
- *Protocolos enrutando:* Configuración correcta y actualizada del enrutador para cada protocolo enrutado.
- *Protocolos Puenteados:* Existencia de filtros configurados en los puentes y una copia de estas configuraciones.
- *Puntos de contacto a redes externas:* Conocimiento del protocolo utilizado para cada conexión externa.
- *Parámetros de desempeño de red:* Se cuenta con registro del comportamiento y desempeño normales en diferentes momentos del día, para poder comparar los problemas actuales con los parámetros de desempeño establecidos (línea de base).

De esta manera se podrá recuperar de una falla más rápido y con mayor facilidad que si no se esta prevenido.

6.3 Herramientas para resolución de problemas

6.3.1 Comandos de diagnostico del enrutador

Los enrutadores proporcionan comandos de ayuda para el monitoreo y la resolución de problemas de la interconectividad de redes. A continuación se mencionan:

- Los comandos *ping* ayudan a determinar la conectividad entre dispositivos de red.
- Los comandos *trace* proporcionan un método para determinar la ruta por medio de la cual los paquetes llegan a su destino de un dispositivo a otro.

6.3.1.1 Uso del comando ping

Para revisar la accesibilidad del host y la conectividad de la red, se debe utilizar el comando de ejecución a nivel de usuario *ping* o el comando de ejecución privilegiada *ping*. Después de haber iniciado una sesión en el enrutador o en el servidor de acceso, ingresar automáticamente al modo de comandos para usuario. Los comandos disponibles a nivel de usuario son un subconjunto de los que se tienen a nivel privilegiado. En general, los comandos para usuario permiten conexion a dispositivos remotos, cambiar temporalmente las especificaciones de la terminal, realizar pruebas básicas y listar información del sistema. El comando ping puede emplearse para confirmar la conectividad de red básica en redes AppleTalk, ISO CLNS, IP, Novell, Apollo, VINES, DECnet o XNS.

Para IP, el comando *ping* envía mensajes de eco ICMP (Protocolo de Mensajes de Control en Internet). ICMP es el protocolo Internet que reporta errores y proporciona información relevante sobre direccionamiento de paquetes IP. Si una estación recibe un mensaje de eco ICMP, entonces envía un mensaje de respuesta de eco ICMP de regreso a su origen.

El modo de comandos extendido de *ping* permite especificar las opciones de encabezado IP soportadas. Esto permite al enrutador realizar un rango más amplio de opciones de prueba.

Es recomendable emplear el comando *ping* cuando la red está funcionando de manera adecuada, a fin de observar la manera en que funciona dicho comando bajo condiciones normales y tener algo contra qué comparar cuando se presentan problemas.

6.3.1.2 Uso del comando trace

El comando para usuario *trace* descubre la ruta que siguen los paquetes de un enrutador cuando viajan hacia su destino. El comando privilegiado *trace* permite especificar las opciones de encabezado de IP soportadas, lo que a su vez permite que el enrutador realice un rango más amplio de opciones de prueba.

El comando *trace* trabaja empleando el mensaje de error generado por los enrutadores cuando un datagrama excede su valor TTL (tiempo de vida). Primero se envían datagramas de prueba con un valor TTL de 1. Esto causa que el primer enrutador descarte los datagramas de prueba y devuelva mensajes de error de "exceso de tiempo". El comando *trace* posteriormente envía varias pruebas y despliega el tiempo del viaje redondo para cada uno. Después de la tercera prueba el TTL se va incrementando en 1.

Cada paquete saliente puede dar como resultado uno o dos mensajes de error. Un mensaje de error "tiempo excedido" indica que un enrutador intermedio ha visto y descartado el datagrama de prueba. Un mensaje de "puerto inalcanzable" indica que el nodo de destino ha recibido el datagrama de prueba y lo ha descartado debido a que no pudo entregar el paquete a una aplicación. Si el tiempo de espera establecido se agota antes de que llegue una respuesta, *trace* imprime un asterisco (*).

El comando *trace* termina cuando el destinatario responde, cuando excede el TTL máximo o cuando el usuario interrumpe la búsqueda de una ruta mediante la secuencia de escape.

Al igual que como sucede con *ping*, es recomendable utilizar el comando *trace* cuando la red está funcionando adecuadamente para ver la manera en que funciona el comando bajo condiciones normales, y así tener referencia con qué comparar cuando se presenten problemas.

6.3.2 Herramientas de terceros para la resolución de problemas

En ocasiones las herramientas de diagnostico de terceros pueden ser más útiles que los comandos integrados en el enrutador. Por ejemplo, la conexión de un analizador de red es menos intrusa y es más probable que produzca información útil sin interrumpir la operación del enrutador. A continuación se enuncian algunas herramientas típicas de terceros usadas en la resolución de problemas de red:

- Los medidores de voltaje y resistencia, los multímetros digitales y los probadores de cables son útiles para probar la conectividad física del tendido de cables.
- Los TDRs (reflectómetros de dominio de tiempo) y los OTDRs (reflectómetros ópticos de dominio de tiempo) son dispositivos que ayudan en la localización de rupturas de cables, falta de correspondencia de impedancias y otros problemas físicos del cableado.
- Las cajas de derivación y las fox boxes son útiles para la solución de problemas en interfaces periféricas.
- Los analizadores de red, decodifican problemas en las siete capas OSI y pueden identificarlos automáticamente en tiempo real, proporcionando una visión clara de la actividad de la red y clasificando los problemas de acuerdo a su nivel crítico.

6.3.2.1 Medidores de voltaje y resistencia, multímetros digitales y los probadores de cables

Estos dispositivos son el nivel inferior del espectro de herramientas para la prueba de cables y miden parámetros tales como el voltaje AC y DC, corriente, resistencia capacitancia y continuidad del cable. Son empleados para revisar la conectividad física.

Los probadores de cables (escáneres) también permiten revisar la conectividad física, los hay para cables STP, UTP y cables 10BaseT, coaxial y bicoaxial (twinax). Estos escáneres son capaces de realizar cualquiera de las siguientes funciones:

- Probar y reportar las condiciones del cable, incluyendo diafonía cercana al extremo (NEXT), atenuación y ruido.
- Realizar funciones de TDR, monitoreo de tráfico y mapa de asignación de terminales.
- Desplegar información de la capa MAC a cerca del tráfico de LAN, proporcionar estadísticas como el uso de la red y las tasas de error de paquetes y realizar pruebas de protocolo limitadas (por ejemplo, pruebas TCP/IP como ping).

Se dispone de equipo de pruebas similar para los cables de fibra óptica. Debido al alto costo relativo de este cable y su instalación, debe probarse antes (pruebas en el carrete) y después de la instalación. La prueba de continuidad de la fibra requiere una fuente de luz visible o un reflectómetro. Las fuentes de luz deben ser capaces de proporcionar luz en las tres longitudes de onda predominantes, 850, 1300 y 1550 nm, se emplean con medidores de potencia que pueden medir las mismas longitudes de onda, probar la atenuación y devolver la pérdida de transmisión en la fibra.

6.3.2.2 TDRs y OTDRs

En la parte más alta del espectro de las pruebas de cable están los TDRs. Estos dispositivos pueden localizar rápidamente circuitos abiertos y en corto, ondulaciones, enroscaduras, dobleces agudos, falta de correspondencia de impedancia y otros defectos en cacles metálicos.

Un TDR funciona mediante el “rebote” de una señal en el extremo del cable, puede medir la distancia del cable, algunos pueden calcular la tasa de propagación con base en una longitud de cable configurada. Las roturas, cortos y otros problemas reflejan la señal a diferentes longitudes, dependiendo del problema. Un TDR mide que tanto tiempo necesita la señal para reflejarse y calcula la distancia hacia la falla en el cable.

La medición de la fibra óptica se realiza con un OTDR, miden con precisión la longitud de la fibra, localiza rupturas de la fibra, mide su atenuación y las pérdidas de las uniones y conectores.

6.3.2.3 Cajas de derivación, fox boxes y BERT/BLERT (probadores de tazas de error de bit/bloque)

Son herramientas de prueba de interfaz digital que se emplean para medir las señales digitales presentes en los equipos de terminal de datos, equipos de comunicaciones de datos e interfaces periféricas. Estos dispositivos pueden monitorear las condiciones de la línea de datos, analizar y atrapar datos, así como diagnosticar problemas comunes en los sistemas de comunicaciones de datos. Es posible examinar el tráfico del DTE a través del DCE para ayudar en el aislamiento de problemas, identificar patrones de bits y asegurarse de que se haya instalado el cableado adecuado. Estos dispositivos no son capaces de probar señales de medios tales como Ethernet, Token Ring o FDDI.

6.3.2.4 Monitores de red

Los monitores de red llevan la cuenta de manera continua de los paquetes que cruzan una red, proporcionando una imagen precisa de la actividad de ésta en cualquier momento, o un registro histórico de la actividad de la red a lo largo de un periodo. No decodifican el contenido de las tramas de datos. Son útiles para determinar la línea de base y para ello se muestra la actividad de la red durante un periodo para establecer un perfil de desempeño normal.

Recolectan información tal como el tamaño de paquetes, la cantidad de paquetes, los paquetes con errores, el uso general de una conexión, la cantidad de hosts y sus direcciones MAC, y detalles acerca de la comunicación entre los hosts y otros dispositivos. Estos datos se pueden utilizar para crear perfiles de tráfico en la LAN, así como para ayudar en la localización de sobrecargas de tráfico, planear la expansión de la red, detectar intrusos, establecer el desempeño de línea de base y distribuir el tráfico de manera más eficiente.

6.3.2.5 Analizadores de Red

Un analizador de red (llamado también *analizador de protocolos*) decodifica las diversas capas de protocolo en una trama de registro y las presenta como abreviaturas o resúmenes legibles, detallando la capa que está involucrada (física, enlace de datos, etc.) y para que sirve cada byte o contenido de byte.

La mayoría de los analizadores de red pueden realizar muchas de las siguientes funciones:

- Filtrar tráfico que satisfaga determinado criterio, para que, por ejemplo, se pueda capturar todo el tráfico hacia y desde un dispositivo particular.
- Anotar la hora de todos los datos capturados.
- Presentar las capas de protocolos en forma fácilmente legible.
- Generar tramas y transmitirlas en la red.
- Incorporar un sistema “experto” en donde el analizador Utilizar un conjunto de reglas, combinadas con información acerca de la configuración y operación de la red, para diagnosticar, resolver o proporcionar soluciones potenciales a los problemas de red.

6.4 Resolución de problemas de Ethernet

La tabla 1 proporciona procedimientos para resolución de problemas comunes asociados a los medios en Ethernet:

Problema de Medios	Acciones Sugeridas
Ruido excesivo	Paso 1. Hacer una revisión física de los cables para determinar si están dañados. Paso 2. Buscar terminadores dañados que causen reflexión de señal. Paso 3. Si se esta usando 1000baseTX, asegurar de que se esta empleando cable categoría 5 y no otro tipo.
Colisiones excesivas	Paso 1. Utilizar un equipo de medición, por ejemplo un reflectómetro, para encontrar cualquier cable Ethernet sin terminación. Paso 2. Buscar cables transceptores dañados o “mordidos” que esten conectados aun host. (Esto puede requerir la inspección de host por host o el uso de un analizador de protocolos).
Exceso de tramas de tamaño pequeño (runt)	En un entorno Ethernet compartido, las tramas de tamaño pequeño son causadas, por lo general, por colisiones. Si la tasa de colisiones es alta, consultar el problema “colisiones excesivas”, que se mostró anteriormente en la tabla. Si las tramas de tamaño excesivo aparecen cuando las colisiones no son altas, o en un entorno Ethernet conmutado, son consecuencia de transmisiones interrumpidas o por software dañado en una tarjeta de interfaz de red. Utilizar un analizador de protocolos para tratar de determinar las direcciones del origen de las tramas de tamaño pequeño.
Colisiones tardías (Es aquella que ocurre más allá de lol primeros 64 bytes de una trama Ethernet)	Paso 1. Utilizar un analizador de protocolos para revisar colisiones tardías. Estas nunca deben ocurrir en na red Ethernet correctamente diseñada. Suceden generalmente cuando los cables Ethernet son demasiado largos o cuando hay demasiados repetidores en la red. Paso 2. Revisar la cobertura de red y asegurarse de que esté dentro de las especificaciones.
No hay integridad del enlace en 10BaseT, 100BaseT4 o 100baseTX	Paso 1. Asegurarse de no estar usando 100BaseT4 cuando sólo se dispone de dos pares de alambres. 100aseT4 requiere de cuatro pares. Paso 2. Revisar si hay falta de correspondencia entre 10BaseT, 100BaseT4 o 100BaseTX (por ejemplo, una tarjeta diferente del puerto de un concentrador). Paso 3. Determinar si hay conexión cruzada (por ejemplo, asegurarse de que no se emplean cables rectos entre una estación y el concentrador). Paso 4. Revisar si hay ruido excesivo (ver el problema “ruido excesivo”, que se mostró anteriormente en esta tabla).

Tabla 1. Procedimientos para resolución de problemas comunes en medios Ethernet

6.5 Resolución de problemas de TCP/IP

A continuación se presenta información de resolución de problemas de conectividad y rendimiento relacionados con TCP/IP. Este tema se concentra en problemas generales de TCP/IP. Esta sección cubre los aspectos de red más comunes en redes IP:

- TCP/IP: El host local no tiene acceso al host remoto
- TCP/IP: Las rutas captadas son del protocolo o interfaz equivocados
- TCP/IP: El enrutamiento no funciona en forma adecuada en una interfaz nueva
- TCP/IP: Las conexiones del host fallan al usar ciertas aplicaciones
- TCP/IP: Problemas en el envío de BOOTP y otras difusiones UDP
- TCP/IP: Rendimiento deficiente

Los síntomas descritos son genéricos y pertenecen a problemas generales de redes TCP/IP.

6.5.1 TCP/IP: El host local no tiene acceso al host remoto

Síntoma. Los hosts de una red no pueden comunicarse con hosts de una red remota. Las redes están separadas por uno o más enrutadores y podrían incluir WANs y otros enlaces. En los enrutadores operan uno o más protocolos de enrutamiento.

Posible problema	Solución
No esta especificada la puerta de enlace predeterminada o está mal configurada en el host local o remoto	Si los hosts no operan con enrutamiento, debe configurarse una puerta de enlace predeterminada Paso 1. Determinar si los hosts local y remoto tienen especificada una puerta de enlace predeterminada. Paso 2. Si es incorrecta la especificación de la puerta de enlace predeterminada, o si no existe, se debe agregar una en el host local. En donde la dirección IP de la puerta de enlace predeterminada (el enrutador local al host). Tal vez se necesite reiniciar el host para que surta efecto este cambio. Paso 3. Se recomienda especificar una puerta de enlace predeterminada como parte del proceso de arranque.
Faltan rutas predeterminadas o están mal configuradas	Paso 1. Si el host opera con enrutamiento se deberá verificar la tabla de enrutamiento del host. Paso 2. La ruta predeterminada debe apuntar al enrutador que tiene la ruta al host remoto. Si no hay un registro de ruta predeterminada, configurar de forma manual la puerta de enlace predeterminada.

Posible problema	Solución
La tabla DNS del host está incompleta	Si el DNS recibe una solicitud de búsqueda de un nombre de host que no está en su cache, no puede responder a la solicitud y el cliente no puede establecer una conexión. Paso 1. Si el resultado es un mensaje de host no encontrado, pero se puede abrir la conexión usando la dirección IP del host en vez de su nombre, probar conectarse a otros hosts usando sus nombres. Si se puede abrir conexiones a otros hosts usando sus nombres, entonces podría estar incompleta la tabla del host. Agregar asignaciones nombre de host-dirección al caché DNS, para cada host de su red. Paso 2. Si no se puede abrir ninguna conexión usando nombres de host, podría no estar operando DNS. Para información sobre resolución de problemas consultar el siguiente problema, “No esta operando DNS”.
No está operando DNS	Si se trata de un host no encontrado, pero se puede abrir la conexión usando la dirección IP del host, podría no estar operando el DNS. Consultar la documentación de software DNS o al administrador de sistemas para información sobre la configuración y activación del DNS.
No esta habilitado el enrutamiento en uno o más enrutadores	Paso 1. Usar el comando trace para aislar el enrutador (o enrutadores) con problemas. Paso 2. Al encontrar sospechoso, Determinar si están habilitados en él los procesos de enrutamiento. Verificar si la tabla de enrutamiento contiene la información de enrutamiento. Paso 3. Si no se está intercambiando la información de enrutamiento, Verificar protocolo de enrutamiento debe estar habilitado. Paso 4. Si no está habilitado el enrutamiento en el enrutador (o enrutadores), habilitar, el protocolo de enrutamiento adecuado. Paso 5. En el modo de configuración del enrutador asocie las redes con el proceso de enrutamiento, según sea aplicable.
Esta mal configurado el enrutamiento en uno o más enrutadores	Resumir los síntomas específicos y resolver el problema utilizando los procedimientos descritos más adelante.

Tabla 2. El host local no tiene acceso al host remoto

6.5.2 TCP/IP: Las rutas captadas son del protocolo o interfaz equivocados

Síntoma: Las redes que deben alcanzarse a través de una interfaz aparecen en la tabla de enrutamiento para ser alcanzadas por otra interfaz distinta. Este problema ocurre sólo en un ambiente de múltiples protocolos.

Posible problema	Solución
El horizonte dividido esta inhabilitado	Paso 1. Verificar la configuración del enrutador. Paso 2. Asegurarse de que este habilitado el horizonte dividido. Paso 3. Si no está habilitado el horizonte dividido, habilitarlo en alguna de las interfaces del enrutador remoto. Para todas las interfaces LAN, la especificación predeterminada del horizonte dividido es habilitada. Sin embargo, para interfaces WAN multipunto configuradas con X.25, Frame Relay o encapsulamiento SMDS (Servicio de Conmutación de datos Multimeabit), la especificación predeterminada del horizonte dividido se encuentra deshabilitada.

Tabla 3. Rutas captadas del protocolo o interfaz equivocada

6.5.3 TCP/IP: El enrutamiento no funciona en forma adecuada en una interfaz nueva

Síntoma: se agrega una nueva interfaz a un enrutador, pero cuando se configura el enrutamiento, éste no funciona adecuadamente en la nueva interfaz.

Posible problema	Solución
No opera el protocolo LAN o la interfaz	Paso 1. Verificar que la interfaz no se encuentre desactivada por el administrador. Paso 2. Si esta desactivada por el administrador, activarla. Paso 3. Si aún no opera la interfaz, podría haber un problema de hardware o medios.
Ho hay interfaces activas configuradas con una dirección IP (sólo OSPF)	OSPF usa como identificar del enrutador una dirección IP de alguna interfaz del enrutador. Por lo tanto, para configurar el protocolo OSPF en un enrutador, se necesita por lo menos una interfaz activa configurada con una dirección IP. Paso 1. Verificar que en el enrutador haya una interfaz de enrutador activa y configurada con una dirección IP. Paso 2. Si no hay una interfaz activa con una dirección IP, configurar una.

Tabla 4. El enrutamiento no funciona en forma adecuada en una interfaz nueva

6.5.4 TCP/IP: Las conexiones del host fallan el usar ciertas aplicaciones

Síntoma: Los intentos de conexión utilizando ciertas aplicaciones tienen éxito, mientras que usando otras aplicaciones fallan.

Posible problema	Solución
Listas de acceso u otros filtros mal configurados	Paso 1. En modo configuración, Revisar cada enrutador que se encuentre en la trayectoria al host. Ver si hay listas de acceso IP configuradas en el enrutador. Paso 2. Si hay listas de acceso IP habilitadas en el enrutador, inhabilitarlas empleando los comandos adecuados. Una lista de acceso podría estar filtrando tráfico de un puerto TCP o UDP. Paso 3. Después de inhabilitar todas las listas de acceso en el enrutador, Determinar si la aplicación en cuestión opera normalmente. Paso 4. Si la aplicación opera con normalidad, es probable que una lista de acceso este bloqueando tráfico. Paso 5. Para aislar la lista con el problema, habilitar una a una las listas de acceso hasta que la aplicación ya no funcione. Revisar la lista de acceso con problema para determinar si está filtrando tráfico desde cualquier puerto TCP o UDP. Paso 6. Si la lista de acceso deniega puertos específicos TCP o UDP, se debe asegurar de que no se deniegue el puerto utilizado por la aplicación en cuestión. Paso 7. Si se modificó una lista de acceso, habilitar la lista para ver si la aplicación aún puede operar normalmente. Paso 8. Si la aplicación opera en forma normal, realizar los pasos anteriores para aislar cualquier otra lista de acceso con problemas hasta que la aplicación opere con todas las listas de acceso habilitadas.

Tabla 5. Las conexiones del host fallan al usar ciertas aplicaciones

6.5.5 TCP/IP: problemas en el envió de BOOTP y otras difusiones UDP

Síntoma: Se presentan problemas al reenviar BOOTP u otros paquetes de difusión UDP. Las difusiones UDP enviadas desde hosts de la red no son reenviadas por los enrutadores. No se pueden arrancar las estaciones de trabajo sin disco.

Posible problema	Solución
Se están enviando difusiones UDP a través de puertos no predeterminados	Especificar una dirección IP asegura que se reenvíen las difusiones sólo desde ciertos puertos UDP predeterminados: Las difusiones UDP reenviadas desde otros puertos requieren una mayor configuración.
El reenvío de difusiones UDP está inhabilitado en puertos UDP específicos	Paso 1. Verificar en la configuración del enrutador que no este inhabilitado el envío de tráfico UDP en puertos específicos. Paso 2. Si están inhabilitadas las difusiones de UDP en puertos UDP específicos, habilitar otra vez las difusiones UDP, BOOTP y DNS.
Las listas de acceso u otros filtros están mal configurados	Paso 1. Revisar la configuración de cada enrutador en la trayectoria al host. Ver si hay listas de acceso configuradas en el enrutador. Paso 2. Si hay listas de acceso habilitadas en el enrutador, inhabilitarlas usando los comandos correspondientes. Paso 3. Después de inhabilitar todas las listas de acceso, Determinar si las difusiones BOOTP u otras difusiones UDP se reenvían normalmente. De no ser así, es probable que una lista de acceso esté bloqueando el tráfico. Paso 4. Para aislar la lista de acceso con el problema, habilitar una por una las listas de acceso hasta que ya no se reenvíen las difusiones. Paso 5. Revisar la lista de acceso con el problema para ver si está filtrando tráfico de cualquier puerto UDP. Si una lista de acceso deniega puertos UDP específicos, asegurarse que no deniegue puertos utilizados para reenviar el tráfico de las difusiones en cuestión. Paso 6. Si se modificó una lista de acceso, habilitarla para ver si el reenvío de difusiones continúa normalmente. Paso 7. Si los problemas persisten, realizar los pasos anteriores sobre los enrutadores en la trayectoria hasta que todo el tráfico de difusiones se reenvíe en forma correcta.

Tabla 6. Problemas en el reenvío de BOOTP y otras difusiones UDP

6.5.6 TCP/IP: Rendimiento deficiente

Síntoma: El rendimiento es lento en uno o más hosts de la red. Las conexiones a servidores emplean un tiempo excesivo para establecerse.

Posible problema	Solución
DNS no está configurado para búsquedas inversas	Si el servidor DNS no está configurado para realizar búsquedas inversas, los intentos de búsquedas inversas por parte de sistemas finales agotaran su tiempo de consulta. Esto puede provocar demoras excesivas a los hosts que intentan establecer conexiones. Para mayor información sobre cómo configurar en forma adecuada el DNS para búsquedas inversas, consultar la documentación de su software DNS.
Tabla de hosts DNS incompleta	Si la tabla de hosts DNS está incompleta, las búsquedas inversas no tendrán éxito y provocarán que se agote el tiempo y se generen demoras. Se debe Agregar asignaciones dirección-nombre de host a la tabla de hosts DNS para cada uno de los hosts de la red.

Tabla 7. Rendimiento deficiente

6.6 Resolución de problemas de línea serial

6.6.1 Uso de pruebas ping extendidas

EL comando ping es una prueba útil que está disponible en muchos dispositivos para interconectividad de redes y en muchos otros hosts. A esta herramienta de diagnostico también se le conoce como petición de eco ICMP.

En general, las pruebas ping de línea serial se realizan de la siguiente manera:

Paso 1. Poner la CSU (Unidad de Servicio de Canal) o DSU (Unidad de Servicio Digital) en modo ciclo de retorno local.

Paso 2. Configurar el modo ping extendido para que envíe patrones de datos y tamaños de paquetes diferentes. Determinar si se han incrementado los errores a la entrada. Si no se han incrementado, es probable que el hardware local (DSU, cable, tarjeta de interfaz de enrutador) esté en buenas condiciones.

Paso 3. Si se supone que está secuencia de pruebas fue precedida por la aparición de una gran cantidad de errores CRC y de entramado, es probable que haya un problema de reloj. Revisar la CSU o DSU para ver si hay algún problema de temporización.

Paso 4. Si se determinó que la configuración de reloj es correcta y está operando adecuadamente, ponga la CSU o DSU en modo de ciclo de retorno remoto.

Paso 5. Repetir la prueba ping y vea si hay cambios en las estadísticas de errores de entrada.

Paso 6. Si se incrementan los errores de entrada, entonces hay un problema en la línea serial o en la CSU/DSU (DTE, en la norma europea). Se debe poner en contacto con el proveedor de servicios WAN y cambiar la CSU o DSU. Si persisten los problemas ponerse en contacto con el representante de soporte técnico.

6.6.2 Resolución de problemas de reloj

Los conflictos de reloj en las conexiones seriales pueden provocar pérdidas crónicas del servicio de conexión o degradación en el desempeño. En términos generales, los problemas de reloj en las interconexiones WAN pueden atribuirse a alguna de las siguientes causas:

- Configuración incorrecta de la DSU
- Configuración incorrecta de la CSU
- Cables fuera de especificación
- Conexiones ruidosas o deficientes en el panel de parcheo
- Varios cables conectados juntos

6.6.2.1 Detección de problemas de reloj

Para detectar conflictos de reloj en una interfaz serial, se buscan errores a la entrada de la manera siguiente:

Paso 1. Verificar la configuración de las interfaces seriales en los enrutadores en ambos extremos del enlace.

Paso 2. Examinar si existen errores de CRC, de entramado y de abortos.

Paso 3. Si alguno de estos pasos indica errores que excedan un rango aproximado de 0.5% a 2.0% del tráfico de la interfaz, es probable que existan problemas de reloj en algún lugar de la WAN.

Paso 4. Aislar la fuente de los problemas de reloj como se indica en la siguiente sección, “Aislamiento de los problemas de reloj”

Paso 5. Poner en derivación o repare cualquier panel de parcheo con fallas.

6.6.2.2 Aislamiento de los problema de reloj

Si se determino que los conflictos de reloj son la causa más probable de los errores a la entrada, el uso del siguiente procedimiento ayudará a aislar la fuente de tales errores.

Paso 1. Realizar una serie de pruebas ping y de ciclo de retorno (tanto locales como remotas) como se describe en la sección “Pruebas de ciclo de retorno de CSU y DSU”, que se trata posteriormente ene este capítulo.

Paso 2. Determinar si el problema está en algún extremo de la conexión o si está en la línea. En el modo de ciclo de retorno local ejecutar pruebas ping con diferentes patrones y tamaños. El uso de un solo patrón y tamaño de paquete podría no forzar la aparición de errores, en particular cuando el problema es un cable serial hacia el enrutador o CSU/DSU.

Paso 3. Determinar si se están incrementando los contadores de errores a la entrada y dónde se están acumulando. Si los errores a la entrada se están acumulando en ambos extremos de la conexión, el problema más probable es el reloj de la CSU. Si sólo un extremo está experimentando errores a la entrada, tal vez haya un problema de reloj de la DSU o de cableado. Los abortos en un extremo indican que el otro extremo está enviando información errónea o que hay un problema de línea.

6.6.2.3 Soluciones para los problemas de reloj

Posible problema	Solución
Configuración incorrecta de la CSU	Paso 1. Determinar si las CSUs que están en ambos extremos coinciden en la fuente del reloj (local o de línea). Paso 2. Si las CSUs no coinciden, configurarlas para que lo hagan (por lo general, la línea es la fuente) Paso 3. Revisar la especificación LBO (Line Built Out) en la CSU para asegurarse que la impedancia concuerde con la de la línea física. Para información de la configuración de la CSU, consultar la documentación de hardware de la CSU.
Configuración incorrecta de la DSU	Paso 1. Determinar si las DSUs de ambos extremos tienen habilitado el modo SCTE. Paso 2. Si SCTE no está habilitado en ambos extremos de la conexión, Habilitarlo. (Se debe activar SCTE para cualquier interfaz que esté conectada a una línea de 128 kbps o más rápida. SI la DSU no soporta SCTE, ver la sección “Inversión del reloj de transmisión”, que se trata posteriormente en este capítulo.) Paso 3. Asegurarse que se mantenga la densidad de unos. Esto requiere que las DSUs usen los mismos esquemas de entrada y codificación (por ejemplo, ESF y B8ZS) usados por la línea arrendada o el proveedor de servicios de comunicaciones. Revisar con el proveedor de la línea arrendada la información sobre sus esquemas de entramado y codificación. Paso 4. Si el proveedor de servicios de comunicaciones usa codificación AMI, invertir el reloj de transmisión en ambos lados del enlace u operar la DSU en modo bit-stuff. Para información de la configuración de la DSU, consultar la documentación del hardware de la DSU.
El cable hacia el enrutador está fura de especificaciones	Si el cable es de más de 15m de largo, usar uno más corto. Si el cable no tiene blindaje, reemplazarlo con cable blindado.

Tabla 8. Problemas y soluciones de reloj

6.6.2.4 Inversión del reloj de transmisión

Si se esta intentando conexiones seriales a velocidades mayores de 64 kbps con una CSU/DSU que no soporta SCTE, tal vez se tenga que invertir el reloj de transmisión en el enrutador. La inversión del reloj de transmisión compensa los corrimientos de fase entre los datos y las señales de reloj.

El comando específico que se usa para la invertir el reloj de transmisión varía entre plataformas. Para asegurarse de que se está usando la sintaxis de comando correcta para el enrutador, consultar la guía de usuario del enrutador o servidor de acceso y las guías de configuración y referencias de comandos.

6.6.3 Ajuste de búferes

La utilización del ancho de banda a más del 70% da como resultado un desempeño general reducido y puede causar intermitencias en las comunicaciones. Por ejemplo, las transmisiones de archivo DECnet pueden estar fallando a causa de paquetes que se descartan en algún lugar de la red.

Si la situación es bastante mala, se debe incrementar el ancho de banda del enlace. Sin embargo, puede ser que el incremento del ancho de banda no sea necesario o inmediatamente posible. Una forma para resolver los problemas de sobreutilización marginal de la línea serial es controlar la manera en que el enrutador emplea los búferes de datos.

Se puede usar algunas de las tres opciones siguientes para controlar la manera en que se usan los búferes:

- *Ajuste los parámetros asociados con los búferes del sistema.* Hay dos tipos generales de búferes en los enrutadores, de hardware y de sistema. Sólo los búferes de sistema son directamente reconfigurables por los administradores del sistema. Los búferes de hardware se usan específicamente como búferes de recepción y transmisión asociados con cada interfaz y (en ausencia de cualquier configuración especial) son administrados de manera dinámica por el software del sistema mismo. Los búferes de sistema están asociados con la memoria principal del sistema y están asignados a bloques de memoria de diferentes tamaños.
- *Especificar la cantidad de paquetes que se guardan en las colas de entrada o salida (colas de contención).* Las colas de contención son búferes usados por cada interfaz de enrutador para guardar paquetes que llegan o salen. Se puede incrementar la cantidad de paquetes de datos que se guardarán en la cola antes de que el enrutador empiece a descartarlas. Incrementando estas colas en porcentajes pequeños (por ejemplo, 2.5%) hasta que ya no se vean paquetes descartados, el límite predeterminado de la cola de salida es de 100 paquetes.
- *Especificar la prioridad en que el tráfico se pone en la cola para la transmisión (colas de salida con prioridad).* La prioridad en colas es un mecanismo de control basado en una lista que permite que se establezca la prioridad del tráfico con base en la interfaz. La prioridad de colas involucra dos pasos: se crea una lista de prioridad por tipo de protocolo y nivel de prioridad, y se asigna la lista de prioridad a una interfaz específica.

Los comandos de configuración asociados con estas tres opciones se describen en las guías de configuración y referencias de comandos.

6.6.4 Pruebas especiales para línea serial

Además de las capacidades de diagnostico básicas que están disponibles en los enrutadores, se puede usar una variedad de herramientas y técnicas suplementarias para determinar las condiciones de los cables, equipo de conmutación, módems, hosts y hardware de interconectividad remota. Para mayor información, se debe consultar la documentación de la CSU, DSU, analizador serial u otro equipo.

6.6.4.1 Pruebas de ciclo de retorno de CSU y DSU

Si la línea serial está bien, pero el protocolo de línea esta inactivo, se usan las pruebas de ciclo de retorno de CSU/DSU para determinar el origen del problema. Se Realiza primero la prueba de ciclo local y luego la de ciclo remoto. En la Figura 2 se ilustra la topología básica de las pruebas de ciclo de retorno local y remoto de CSU/DSU.

Estas pruebas son genéricas por naturaleza y asumen la conexión del sistema de inteconectividad a una CSU o DSU. Sin embargo, las pruebas son esencialmente las mismas para las conexiones con un multiplexor con funcionalidad CSU/DSU integrada. Debido a que no hay concepto de ciclo de retorno en los entornos de redes de conmutación de paquetes X.25 o Frame Relay, las pruebas de ciclo de retorno no se aplican a las redes X.25 o Frame Relay.

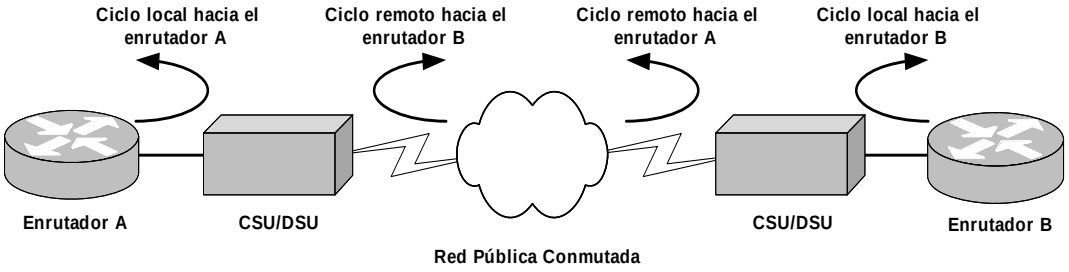


Figura 2. Pruebas de ciclo local y remoto de CSU/DSU

6.6.4.1.1 Pruebas de ciclo de retorno local de CSU y DSU para enlaces HDLC o PPP

A continuación se presenta un procedimiento general para la realización de pruebas de ciclo de retorno junto con las capacidades de diagnóstico de sistema integradas:

Paso 1. Poner la CSU/DSU en modo de ciclo local (consultar la información del fabricante). En el modo de ciclo de reloj se determina el uso de reloj de línea y se fuerza a la DSU a usar el reloj local.

Paso 2. Verificar mediante el comando apropiado si el estado de la línea cambia de “el protocolo de línea está inactivo” a “el protocolo de línea está operando (en ciclo)” o si permanece inactivo.

Paso 3. Si el protocolo de línea se establece cuando la CSU o DSU está en modo de ciclo de retorno local, esto indica que el problema está ocurriendo en el extremo remoto de la conexión serial. Si el estado de la línea no cambia, es posible que haya un problema en el enrutador, en el cable de conexión o en la CSU/DSU.

Paso 4. Si el problema es local, se debe quitar la CSU/DSU del modo de ciclo local. Cuando el protocolo de línea está inactivo, los contadores de monitoreo de la conexión (*keepalive*) no se están incrementando.

Paso 5. Volver a colocar la CSU/DSU en modo de ciclo local. Esto provocará que los paquetes de monitoreo de la conexión comiencen a incrementarse.

Si los valores de monitoreo de la conexión no se incrementan, puede ser un problema de temporización en la tarjeta de interfaz o en la red.

Paso 6. Revisar el enrutador local, el hardware de CSU/DSU y cualquier cable conectado. Asegurarse que los cables tengan la longitud recomendada y de que estén conectados a los puertos adecuados. Cambiar el equipo que este fallando.

6.6.4.2 Pruebas de ciclo de retorno remoto de CSU/DSU para enlaces HDCL o PPP

Si el hardware local esta funcionando adecuadamente, pero todavía no se encuentran problemas cuando se trata de establecer conexiones a través de un enlace serial, se puede emplear la prueba de ciclo de retorno remoto para aislar la causa del problema.

Esta prueba de ciclo remoto asume que se está usando encapsulación HDLC y que se realizó previamente la prueba de ciclo local.

Los pasos que se requieren para realizar la prueba de ciclo de retorno remoto son los siguientes:

Paso 1. Poner la CSU o DSU remota en modo de ciclo de retorno remoto (consultar la información del fabricante).

Paso 2. Usando el comando apropiado, determinar si el protocolo de línea está operando con el estado de la línea indicando “el serial x está operando, el protocolo de la línea está operando (en ciclo)” o si se desactiva la línea, con la condición de estado indicando “el protocolo de línea está inactivo”.

Paso 3. Si el protocolo de línea permanece operando tal vez el problema está en el extremo remoto de la conexión serial (entre la CSU/DSU remota y el enrutador remoto). Realizar pruebas locales y remotas en el extremo remoto para aislar el origen del problema.

Paso 4. Si el estado de la línea cambia a “el protocolo de línea esta inactivo” cuando está activado el modo de ciclo de retorno remoto, asegurarse de que esté manteniendo adecuadamente la densidad de unos. La CSU/DSU debe estar configurada para usar los mismos esquemas de entramado y codificación usados por la línea arrendada u proveedor de servicios de comunicaciones.

Paso 5. Si el problema persiste, ponerse en contacto con su administrador de red WAN o con la organización de servicio WAN.

6.7 Resolución de problemas en redes con bridging transparente

Los puentes transparentes reciben este nombre debido a que su presencia y operación son transparentes ante los hosts de la red. Cuando se encienden, los puentes transparentes aprenden la topología de la red analizando las direcciones de origen de las tramas de entrada de todas las redes conectadas.

A continuación se presenta información sobre la resolución de problemas de conectividad en redes con bridging transparente. Describe síntomas específicos del bridging transparente, los posibles problemas que causen cada síntoma y las soluciones a dichos problemas.

6.7.1 No hay conectividad

Síntoma: el cliente no puede conectarse con el host a través de una red con puente transparente.

Posible problema	Solución
Problema de hardware o medios	Paso 1. Verificar si hay un problema de conectividad. En caso de que lo haya, no se mostrará ninguna dirección MAC en la tabla de bridging. Paso 2. Determinar si esta bien la interfaz y el protocolo de línea. Paso 3. Si la interfaz está inactiva, resolver los problemas del hardware o medios. Paso 4. Si el protocolo de la línea esta inactivo, revisar la conexión física entre la interfaz y la red. Asegurarse de que la conexión esté bien asegurada y que los cables no estén dañados. Si el protocolo de línea está funcionando, pero los contadores de paquetes de entrada y de salida no se están incrementando, revisar los medios y la conectividad del host.
No se intercambian mensajes Hello	Paso 1. Revisar si los puentes se están comunicando entre ellos. Utilizar un analizador de red para ver si están intercambiando tramas hello spanning tree. Paso 2. Si no se están intercambiando mensajes hello, revisar las conexiones físicas y la configuración de software en los puentes.

Posible problema	Solución
Filtros de bridging mal configurados	Paso 1. Determinar si están configurados los filtros del puente, usando comandos de configuración. Paso 2. Desactivar los filtros del puente en las interfaces sospechosas y determinar si vuelve a haber conectividad. Paso 3. Si no se vuelve a tener conectividad, los filtros no son el problema. Si la conectividad se restaura después de la eliminación de filtros, uno o más filtros malos están causando el problema de conectividad. Paso 4. Si existen varios filtros, o filtros que estén empleando listas de acceso con varias instrucciones, aplicar cada filtro individualmente para identificar al filtro con problemas. Revisar la configuración de los filtros de entrada y salida LSAP (Punto de Acceso al Servicio de Enlace) y TYPE, los cuales pueden estarse empleando de manera simultánea para bloquear diferentes protocolos. Paso 5. Modificar cualquier filtro o lista de acceso que esté bloqueando el tráfico. Continuar probando los filtros hasta que todos están activados y las conexiones todavía funcionen.
Colas de entrada y salida llenas	El tráfico excesivo de difusión o difusión restringida puede causar que se desborden las colas de entrada y salida, dando como resultado el descarte de paquetes. Paso 1. Verificar si existen paquetes descartados en la entrada y salida. Dichos paquetes sugieren demasiado tráfico través de los medios. Si la cantidad actual de paquetes en la cola de entrada es constantemente 80%, o más, del tamaño actual de la cola de entrada, puede ser que el tamaño de la cola de entrada requiera ajustarse para acomodar la tasa de paquetes en la entrada. Aunque el número actual de paquetes en la cola de entrada nunca parezca aproximarse al tamaño de está, puede ser que las ráfagas de paquetes estén desbordando la cola. Paso 2. Reducir el tráfico de difusión y de difusión restringida en las redes conectadas implementando filtros de bridging, o segmentar la red utilizando más dispositivos de interconexión de red. Paso 3. Si la conexión es a través de un enlace serial, se tiene que incrementar el ancho de banda, aplicar colas con prioridad, incrementar el tamaño de retención de la cola o modificar el tamaño del búfer del sistema.

Posible problema	Solución
El host está fuera de operación	Paso 1. Verificar y asegurarse que la tabla de bridging incluya las direcciones MAC de los nodos finales conectados. La tabla de bridging comprende las direcciones MAC de origen y destino de los hosts, y se llena cuando los paquetes de origen o destino pasan a través del puente. Paso 2. Si esta faltando cualquier nodo final esperado, revisar el estado de los nodos para verificar que estén conectados y configurados de manera adecuada. Paso 3. Volver a inicializar o reconfigurar los nodos finales las veces que sea necesario y examinar la tabla de bridging.

Tabla 9. Ho hay conectividad

6.7.2 Las sesiones terminan de manera inesperada

Síntoma: Las conexiones en un entorno con bridging transparente se establecen de manera satisfactoria, pero a veces las sesiones terminan abruptamente.

Posible problema	Solución
Retransmisiones excesivas	Paso 1. Utilizar un analizar de red para ver las retransmisiones del host. Paso 2. Si se ven retransmisiones en líneas seriales lentas, se incrementan los temporizadores de transmisión en el host. Para información sobre la configuración de los hosts, consultar la documentación del fabricante. Si se observa retransmisiones en medios LAN de alta velocidad, revisar si hay paquetes enviados y recibidos en orden o descartados por cualquier dispositivo intermedio, tal como un puente o un switch. Resolver los problemas de medios LAN como sea adecuado. Paso 3. Emplear un analizador de red para determinar si disminuye la cantidad de retransmisiones.
Retraso excesivo a través del enlace serial	Incrementar el ancho de banda, aplicar colas con prioridad, incrementar el tamaño de retención de la cola o modificar el tamaño del búfer del sistema.
Varios puentes raíz	Si hay puentes raíz en la red, tal vez cambie periódicamente la raíz del spanning tree, lo que causa que fallen las conexiones. Paso 1. Utilizar un analizador de red para saber si hay varios puentes raíz. Paso 2. Si hay varios puentes raíz en la red eliminar a los puentes extraños y configurar los puentes raíz para que el puente deseado se convierta en raíz.

Tabla 10. Las sesiones terminan en forma inesperada

6.7.3 Se presentan ciclos y ráfagas de difusión

Síntoma: El ciclo de paquetes y las ráfagas de difusión se presentan en entornos con bridging transparente. Las estaciones finales son forzadas a una retransmisión excesiva, causando que se agote el tiempo de sesión o que está sea eliminada.

Por lo general, los ciclos de paquetes son causados por problemas de diseño de red.

Posible problema	Solución
No está implementando el spanning tree	Paso 1. Examinar el mapa de topología de la red para ver si hay posibles ciclos. Paso 2. Eliminar cualquier ciclo que exista o asegurarse de que los enlaces adecuados estén en modo de respaldo. Paso 3. Si persisten las ráfagas de difusión y los ciclos de paquetes, implementar un algoritmo de spanning tree para impedir los ciclos.
Falta concordancia en el algoritmo spanning tree	Paso 1. Verificar que tipo de algoritmo spanning tree se esta usando en cada puente. Paso 2. Asegurarse de que todos los puentes estén ejecutando el mismo algoritmo spanning tree (ya sea DEC o IEEE). Si se están usando algoritmos de ambos tipos, volver a configurar los puentes como convenga, para que todos utilicen el mismo algoritmo spanning tree. Los algoritmos spanning tree DEC e IEEE son incompatibles.
Varios dominios con bridging mal configurados	Paso 1. Verificar que concuerden todos los números de grupo de dominio para los dominios con bridging dados. Paso 2. Si están configurados varios grupos de dominio para el puente, asegurarse de que todas las especificaciones de dominio estén asignadas correctamente. Paso 3. Asegurarse de que no existan ciclos entre dominios con bridging. Un entorno con bridging entre dominios no proporciona prevención de ciclos con base en el spanning tree. Cada domino tiene su propio spanning tree, que es independiente de los que existan en otros dominios.

Tabla 11. Se presentan ciclos y ráfagas de difusión

6.8 Resolución de problemas en los entornos con conmutación LAN

En esta sección se describen síntomas específicos de la conmutación de LAN, los posibles problemas que causen cada síntoma y las soluciones a dichos problemas.

6.8.1 Ho hay conectividad hacia la LAN directamente conectada.

Síntomas: Un switch no puede conectarse a dispositivos de su LAN directamente conectada.

Posible problema	Solución
Cableado con fallas o incorrecto	Paso 1. Revisar si el LED Connected del switch está encendido. Paso 2. Si dicho LED no está encendido, Revisar si está empleando el canle correcto y si está conectado adecuadamente y en forma segura. Por ejemplo, asegurarse de que no está usando un cable cruzado cuando se requiere uno recto, o viceversa. Paso 3. Asegurarse de que el cable este correctamente alambrado. Para obtener información sobre los pines del cable, consultar la guía de usuario del switch. Paso 4. Utilizar un TDR u otro dispositivo para revisión de cable a fin de verificar que el cable no tenga aberturas, cortos u otros problemas. Paso 5. Intercambiar el cable con otro del mismo tipo para ver si dicho cable está mal. Si ahora se pueden realizar las conexiones, la falla es del cable. Paso 6. Reemplazar y corregir el cable con fallas si es necesario.
Problema de alimentación de corriente	Paso 1. Revisar el LED Power. Si no está encendido, asegurarse de que el switch esté enchufado y encendido. Paso 2. Revisar para ver si hay un fusible fundido. Si es así, consultar la guía de usuario del switch para información sobre el reemplazo del fusible.
Problema de Hardware	Paso 1. Revisar si el LED Connected del puerto está encendido. Paso 2. Si dicho LED no está encendido y el cableado está intacto, puede haber un puerto de switch malo u otro problema de hardware. Paso 3. Revisar si el LED Module Enabled para los módulos FDDI y Fast Ethernet está encendido. Paso 4. Si dicho LED no está encendido, quitar el módulo y volverlo a enchufar. Paso 5. Revisar el hardware del switch y reemplazar cualquier componente que falle.

Tabla 12. No hay conectividad hacia la LAN directamente conectada

6.8.2 No hay conectividad hacia la LAN o WAN

Síntoma: Un switch no puede conectarse con dispositivos que están en otra LAN o a través de una LAN. Fallan los intentos para ejecutar ping hacia el switch desde dispositivos remotos o desde el switch hacia dispositivos remotos.

Posible problema	Solución
Dirección IP mal configurada o no especificada	Paso 1. Revisar si hay una dirección IP configurada en el switch. Asegurarse de que hay una dirección IP en el dispositivo desde el cual esta tratando de ejecutar ping hacia el switch. Paso 2. Si la dirección IP está mal configurada o no está especificada en cualquiera de los dispositivos, cambiar o añadir la dirección IP como sea adecuado. Para información sobre la manera de revisar y configurar la dirección IP en el switch, consultar la guía de usuario del switch. Consultar la documentación del distribuidor del otro dispositivo para información sobre la manera de revisar y configurar la dirección IP en ese dispositivo.
Error de configuración de máscara de red	Paso 1. Revisar si se puede ejecutar ping hacia el switch desde un dispositivo en la misma subred. Paso 2. Revisar la máscara de subred en el dispositivo desde el cual está ejecutando ping. Revisar la máscara de subred en el switch. Paso 3. Determinar si la máscara de subred en cualquier dispositivo está especificada incorrectamente. De ser así, configurar el switch o el dispositivo como sea adecuado con la máscara de su subred correcta. Para información sobre la manera de revisar y configurar la máscara de subred en el switch, consultar la guía de usuario del switch. Consultar la documentación del distribuidor del otro dispositivo para información sobre la manera de revisar y configurar la máscara de subred en ese dispositivo.
No hay puerta de enlace predeterminada especificada en el switch o servidor	Paso 1. Revisar si hay una puerta de enlace predeterminada configurada en el switch. Asegurarse de que todos los servidores y demás sistemas finales de la LAN tengan una especificación de puerta de enlace predeterminada. Paso 2. Si cualquiera de estos dispositivos no tiene especificada una puerta de enlace predeterminada, configurar una empleando la dirección IP de una interfaz de enrutador en la LAN directamente conectada. Para información sobre la manera de revisar y configurar la puerta de enlace predeterminada en el switch, consultar la guía de usuario del switch. Consultar la documentación del distribuidor del otro dispositivo para información sobre la manera de revisar y configurar una puerta de enlace predeterminada en esos dispositivos.

Posible problema	Solución
Configuración errónea de VLAN	Paso 1. Asegurarse de que todos los nodos que deben comunicarse estén conectados a puertos de la misma VLAN. Si los puertos están signados a VLANs diferentes, los dispositivos conectados no podrán comunicarse. Paso 2. Si un puerto pertenece a dos o más VLANs, asegurarse de que el puerto en traslape sea el único que las conecte. Si hay otras conexiones, se puede crear una topología de red inestable. Paso 3. Eliminar cualquier conexión extraña entre las dos VLANs.
Opción incorrecta de conector de puerto 25	Si un puerto de switch tiene dos conectores posibles, asegurarse de que la conexión física concuerde con la configurada en la consola de administración.

Tabla 13. No hay conectividad hacia la LAN o WAN

6.8.3 No se puede acceder la administración fuera de banda

Síntoma: La consola de administración fuera de banda del switch es inaccesible.

Posible problema	Solución
Velocidad en baudios mal configurada	Paso 1. Asegurarse de que el switch y la terminal o módem conectados estén configurados para utilizar la misma velocidad en baudios y formato de carácter. En la mayoría de los switches la característica de auto baudios puede hacer concordar la velocidad en baudios de las llamadas en entrada, pero el switch no cambiará su velocidad configurada cuando haga llamadas. Además, dicha característica sólo hará concordar una velocidad menor a la que tiene configurada. Cuando termina una llamada y se desconecta, el switch regresa a la velocidad en baudios configurada por última vez. Paso 2. Pruebe la conexión usando velocidades en baudios diferentes. Para mayor información de la manera de conectar una terminal o módem, consultar la guía de usuario del switch.
Cableado incorrecto	Cuando se conecta un switch directamente a terminales u otras estaciones, es necesario un cable de módem nulo. Cuando se conecta el switch a un módem, es necesario un cable directo

Tabla 14. No se puede acceder la administración fuera de banda

6.9 SNMP (Simple Network Management Protocol)

SNMP (*Simple Network Management Protocol*) es el protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red. El funcionamiento de SNMP es sencillo, como dice el protocolo, aunque su implementación es tremendamente compleja. SNMP utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UPD, sin embargo, el hecho de

usar UDP hace que el protocolo no sea fiable (en UDP no se garantiza la recepción de los paquetes enviados, como en TCP).

El protocolo SNMP está cubierto por un gran número de RFCs, entre ellos el RFC 1157, 1215 (versión 1), del 1441 al 1452 (versión 2), del 2271 al 2275 y del 2570 al 2575 (para SNMP v3).

SNMP se basa en un conglomerado de agentes. Cada agente es un elemento de la red que ofrece unas determinadas variables al exterior, para ser leídas o modificadas. Asimismo, un agente puede enviar "alertas" a otros agentes para avisar de eventos que tengan lugar. Generalmente se llama "gestor" al agente encargado de recibir estos eventos.

El esquema es sencillo, sin embargo su complejidad se incrementa a la hora de definir las variables (y su formato). Las variables ofrecidas para consulta por los agentes SNMP se definen a través de una MIB (*Management Information Base*, Base de Información de Gestión). La MIB (hay sólo una aunque existen múltiples extensiones a ésta) es una forma de determinar la información que ofrece un dispositivo SNMP y la forma en que se representa. La MIB actual es MIB-II y está definida en el RFC 1213, aunque hay múltiples extensiones definidas en otros RFCs. La MIB está descrita en ASN.1 para facilitar su transporte transparente por la capa de red.

Cada agente SNMP ofrece información dentro de una MIB, tanto de la general (definida en los distintos RFCs) como de aquellas extensiones que desee proveer cada uno de los fabricantes. Así, los fabricantes de enrutadores han extendido las MIBs estándar incluyendo información específica de sus equipos.

Con SNMP se puede monitorizar el estado de un enlace punto a punto para detectar cuando está congestionado y tomar así medidas oportunas, se puede hacer que una impresora alerte al administrador de la red cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de un ordenador a través de su agente SNMP, u obligar a la ejecución de comandos (si el agente ofrece las funcionalidades necesarias)

6.9.1 Arquitectura SNMP

Implícita en el modelo de arquitectura del SNMP existe una colección de estaciones de gestión de red y de elementos de red. Las estaciones de gestión de red ejecutan aplicaciones de gestión que monitorizan y controlan los elementos de red. Los elementos de red son dispositivos como hosts, gateways, servidores de terminal, y parecidos, que poseen agentes de gestión para realizar las funciones de gestión de red solicitadas por las estaciones de gestión de red. El SNMP es usado para comunicar información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red.

El SNMP explícitamente minimiza el número y complejidad de las funciones de gestión realizadas por el propio agente de gestión. Esta meta es atractiva al menos en cuatro aspectos:

1. El costo de desarrollo del software del agente de gestión necesario para soportar el protocolo se reduce acordemente.
2. El grado de funciones de gestión soportado remotamente se incrementa, posibilitando un uso completo de los recursos de Internet en la tarea de gestión.
3. El grado de funciones de gestión soportado remotamente se incrementa, imponiendo así las mínimas restricciones posibles en la forma y sofisticación de herramientas de gestión.
4. Los conjuntos simplificados de funciones de gestión son fácilmente entendibles y usados por los creadores de herramientas de gestión de red.

Un segundo objetivo del protocolo es que el paradigma funcional para monitorizar y controlar sea lo suficientemente flexible como para posibilitar aspectos de gestión y operación de la red adicionales y posiblemente no anticipados.

Un tercer propósito es que la arquitectura sea en lo posible independiente de la arquitectura y mecanismos de hosts o gateways particulares.

6.9.1.1 Elementos de la Arquitectura

La arquitectura SNMP formula una solución al problema de gestión de redes en términos de:

a) Alcance de la información de gestión comunicada por el protocolo
b) Representación de la información de gestión comunicada por el protocolo.
c) Operaciones soportadas por el protocolo en la información de gestión.
d) Forma y significado de los intercambios entre entidades de gestión.
e) Definición de las relaciones administrativas entre entidades de gestión.
f) Forma y significado de las referencias a la información de gestión.

6.9.1.1.1 Alcance de la información de gestión

El alcance de la información de gestión transmitida por operaciones del SNMP es exactamente el representado por casos de todos los tipos de objetos no agregados, definidos en el estándar MIB de Internet, o definidos en cualquier otro sitio de acuerdo a las convenciones expuestas en la norma SMI de Internet.

6.9.1.1.2 Representación de la información de gestión

La información de gestión se representa según el lenguaje ASN.1, que es especificado para la definición de tipos no agregados en el SMI. El SNMP utiliza un subconjunto bien definido de dicho lenguaje, incluyendo un subconjunto más complejo para la descripción de objetos gestionados y para describir las unidades de datos de protocolo (PDUs) utilizadas para gestionar esos objetos. Así mismo solo se utiliza un subconjunto de las reglas básicas de codificación del ASN.1, esto es, todas las codificaciones utilizan la forma de longitud definida. Con el deseo de facilitar una futura transición a protocolos de gestión de redes basados en OSI, se procedió a la definición en el lenguaje ASN.1 de una norma SMI de Internet y de un MIB.

6.9.1.1.3 Operaciones soportadas por la información de gestión

El SNMP modela las funciones del agente de gestión como lecturas (get) o escrituras (set) de variables. Esta estrategia posee al menos dos consecuencias positivas:

- Limita el número esencial de funciones de gestión realizadas por el agente de gestión a dos.
- Evita introducir el soporte de comandos de gestión imperativos en la definición del protocolo.

La estrategia se basa en que la monitorización del estado de la red se puede basar a cualquier nivel de detalle en el sondeo (poll) de la información apropiada en la parte de los centros de monitorización. Un número limitado de mensajes no solicitados (traps) guían el objetivo y la secuencia del sondeo.

Las funciones de los pocos comandos imperativos actualmente soportados pueden ser fácilmente implementados en este modelo de modo asíncrono.

6.9.1.1.4 Forma y significado de los intercambios

La comunicación de la información de gestión entre entidades de gestión se realiza en el SNMP por medio del intercambio de mensajes de protocolo. El intercambio de mensajes SNMP sólo requiere un servicio de datagramas poco confiable, y todo mensaje se representa por un único datagrama de transporte.

6.9.1.1.5 Forma y significado de las referencias a objetos gestionados

El SMI requiere que la definición de un protocolo de gestión contemple:

- *Resolución de referencias MIB ambiguas:* Debido a que el alcance de cualquier operación SNMP está conceptualmente confinado a los objetos relevantes a un único elemento de red, y ya que todas las referencias SMI a objetos MIB son por medio de nombres de variables únicos, no hay posibilidad de que una referencia SNMP a cualquier tipo de objeto definido en el MIB se pueda resolver entre múltiples casos de ese tipo.
- *Resolución de referencias MIB en presencia de múltiples versiones MIB:* El objeto referenciado por cualquier operación SNMP es exactamente el especificado como parte de la operación de petición, o en el caso de una operación get-next su sucesor en el conjunto de MIB. En particular, una referencia a un objeto como parte de una versión del MIB estándar de Internet, no se aplica a ningún objeto que no sea parte de dicha versión, excepto en el caso de que la operación sea get-next, y que el nombre del objeto especificado sea el último léxico gráficamente entre los nombres de todos los objetos presentados como parte de dicha versión.
- *Identificación de casos particulares de tipos de objetos definidos en el MIB:* Cada caso de un tipo de objeto definido en el MIB se identifica en las operaciones SNMP por un nombre único llamado su "nombre de variable". En general, el nombre de una variable SNMP es un identificador de objeto de la forma *x.y*, donde *x* es el nombre del tipo de

objeto no agregado definido en el MIB, e *y* es un fragmento de un identificador de objeto que de forma única para dicho tipo de objeto, identifica el caso deseado. Esta estrategia de denominación admite la completa explotación de la semántica de la PDU GetNextRequest, dado que asigna nombres para variables relacionadas de forma que sean contiguas en la ordenación lexicográfica de todas las variables conocidas en el MIB.

6.9.2 Especificaciones del Protocolo

El protocolo de administración de red es un protocolo de aplicación por el que las variables del MIB de un agente pueden ser inspeccionadas o alteradas.

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU. Estos datagramas no necesitan ser mayores de 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores.

Todas las implementaciones del SNMP soportan 5 tipos de PDU:

- GetRequest-PDU
- GetNextRequest-PDU
- GetResponse-PDU
- SetRequest-PDU
- Trap-PDU

6.9.2.1 Elementos de procedimiento

Se describirán a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Definiremos *dirección de transporte* como una dirección IP seguida de un número de puerto UDP (Si se está usando el servicio de transporte UDP).

Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1
2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autentificación. Este servicio generará en respuesta otro objeto en ASN.1
3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autentificación y el nombre de comunidad
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

1. Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.

2. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.
3. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autentificación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (trap), descarta el datagrama y no realiza más acciones.
4. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta ahora.

6.9.2.1.1 Estructura de una PDU

Los datos que incluye una PDU genérica son los siguientes:

- *RequestID*: Entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco confiables.
- *ErrorStatus*: Entero que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente:
  - noError (0)
  - tooBig (1)
  - noSuchName (2)
  - badValue (3)
  - readOnly (4)
  - genErr (5)

- *ErrorIndex*: entero que en caso de error indica qué variable de una lista ha generado ese error.
- *VarBindList*: Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aún así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.

6.9.2.1.1.1 GetRequest-PDU y GetNextRequest-PDU

Son PDUs que solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables son las que se encuentran en la lista VarBindList; en el de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, GetNextRequest-PDU es útil para confeccionar tablas de información sobre un MIB. Siempre tienen a cero los campos ErrorStatus y ErrorIndex. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Estas PDUs siempre esperan como respuesta una GetResponse-PDU.

6.9.2.1.1.2 SetRequest-PDU

Ordena a la entidad destino poner a cada objeto reflejado en la lista VarBindList el valor que tiene asignado en dicha lista. Es idéntica a GetRequest-PDU, salvo por el

identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta una GetResponse-PDU.

6.9.2.1.1.3 GetResponse-PDU

Es una PDU generada por la entidad de protocolo sólo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Contiene o bien la información requerida por la entidad destino o bien una indicación de error.
Cuando una entidad de protocolo recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, sigue las siguientes reglas:

1. Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de GetNextRequest-PDU) no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.
2. De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.
3. Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.
4. Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).
5. Si el valor de algun objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 5 (genErr), y el campo ErrorIndex indicando el objeto de la lista que ha originado el error.

Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una GetResponse-PDU de las siguientes características:

- Si es una respuesta a una GetResponse-PDU, tendrá la lista varBindList recibida, pero asignando a cada nombre de objeto el valor correspondiente.
- Si es una respuesta a una GetNextResponse-PDU, tendrá una lista varBindList con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto con cada nombre, aparecerá su correspondiente valor.
- Si es una respuesta a una SetResponse-PDU, será idéntica a esta, pero antes la entidad asignará a cada variable mencionada en la lista varBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de estos casos, el valor del campo ErrorStatus es 0 (noError), igual que el de ErrorIndex. El valor del campo requestID es el mismo que el de la PDU recibida.

6.9.2.1.1.4 Trap-PDU

Es una PDU que indica una excepción o trampa. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una Trap-PDU, presenta sus contenidos a su entidad de aplicación SNMP.
Los datos que incluye una Trap-PDU son los siguientes:

- *enterprise*: tipo de objeto que ha generado la trampa.
- *agent-addr*: dirección del objeto que ha generado la trampa.
- *generic-trap*: entero que indica el tipo de trampa. Puede tomar los siguientes valores:
  - coldStart (0)
  - warmStart (1)
  - linkDown (2)
  - linkUp (3)
  - authenticationFailure (4)
  - egpNeighborLoss (5)
  - enterpriseSpecific (6)
- *specific-trap*: entero con un código específico.
- *time-stamp*: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.
- *variable-bindings*: lista tipo varBindList con información de posible interés.

Dependiendo del valor que tenga el campo generic-trap, se iniciarán unas u otras acciones:

- *Trampa de arranque frío* (coldStart): La entidad de protocolo remitente se está reinicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada.
- *Trampa de arranque caliente* (warmStart): La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.
- *Trampa de conexión perdida* (linkDown): La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Esta Trap-PDU contiene como primer elemento de la lista variable-bindings el nombre y valor del interfaz afectado.
- *Trampa de conexión establecida* (linkUp): La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable-bindings es el nombre y el valor del interfaz afectado.
- *Trampa de fallo de autentificación* (authenticationFailure): La entidad de protocolo remitente es la destinataria de un mensaje de protocolo que no ha sido autentificado.
- *Trampa de pérdida de vecino EGP* (egpNeighborLoss): Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista variable-bindings es el nombre y el valor de la dirección del vecino afectado.
- *Trampa específica* (enterpriseSpecific): La entidad remitente reconoce que ha ocurrido algún evento específico. El campo specific-trap identifica qué trampa en particular se ha generado.

6.9.3 Ventajas de SNMP

La ventaja fundamental de usar SNMP es que su diseño es simple por lo que su implementación es sencilla en grandes redes y la información de gestión que se necesita intercambiar ocupa pocos recursos de la red. Además, permite al usuario elegir las variables que desea monitorizar sin mas que definir:

- El título de la variable.
- El tipo de datos de las variables.
- Si la variable es de solo lectura o también de escritura.
- El valor de la variable.

Otra ventaja de SNMP es que en la actualidad es el sistema más extendido. La popularidad la ha conseguido al ser el único protocolo que existió en un principio y por ello casi todos los fabricantes de dispositivos como switches y enrutadores diseñan sus productos para soportar SNMP. La posibilidad de expansión es otra ventaja del protocolo SNMP: debido a su sencillez es fácil de actualizar.

6.9.4 Desventajas de SNMP

El protocolo SNMP no es ni mucho menos perfecto. Tiene sus fallos que se han ido corrigiendo. La primera deficiencia de SNMP es que tiene grandes fallos de seguridad que puede permitir a intrusos acceder a información que lleva la red. Todavía peor, estos intrusos pueden llegar a bloquear o deshabilitar los hosts. La solución a este problema es sencilla y se ha incorporado en la nueva versión SNMPv2. Básicamente se han añadido mecanismos para resolver:

- Privacidad de los datos, los intrusos no puedan tomar información que va por la red.
- Autentificación, para prevenir que los intrusos manden información falsa por la red.
- Control de acceso, que restringe el acceso a ciertas variables a determinados usuarios que puedan hacer caer la red.

El mayor problema de SNMP es que se considera tan simple que la información está poco organizada, lo que le hace no muy acertada para gestionar las grandes redes de la actualidad. Esto se debe en gran parte a que SNMP se creó como un protocolo provisional pero que se ha quedado sin ser sustituido por otro de entidad.

De nuevo este problema se ha solucionado con la nueva versión SNMPv2 que permite una separación de variables con más detalle, incluyendo estructuras de datos para hacer más fácil su manejo. Además SNMPv2 incluye 2 nuevas PDUs orientadas a la manipulación de objetos en tablas.

Por tanto, SNMP es un sistema de gestión que se ha quedado anticuado y que necesitaba con urgencia un recambio que ha venido de la mano de la versión 2 del mismo. SNMP ya no es capaz de soportar la intensa actividad que sufren redes como Internet.

6.10 Hojas de trabajo para la resolución de problemas

Para aislar problemas en la red primero se debe recopilar todos los hechos relevantes y luego atacar metódicamente cada sospecha de problema. Las siguientes hojas de trabajo para la resolución de problemas pueden ser de ayuda en este proceso. Se deben usar estas hojas como lineamientos que ayuden en el desarrollo de hojas de trabajo propias, acordes con el entorno de red en cuestión.

1. Síntomas reportados
2. Mapa de la topología de la red
3. Protocolos de red implementados
4. Protocolos enrutados
5. Protocolos puenteados
6. Puntos de contacto con redes externas
7. Equipo de interconexión de red (incluyendo dirección de red, fabricante modelo y función)
8. Nodos de sistemas finales y de interred sospechosos (incluyendo dirección de red, fabricante, modelo y función)
9. Aplicaciones usadas en la red (FTP, sendmail, NFS, Net Ware, etc.)
10. Síntomas y posibles problemas

Síntoma	Posibles problemas

11. Plan de acción para cada problema

Problema	Plan de acción

12. Resultado de las acciones

Problema	Acción	Resultado

Conclusiones

Este trabajo proporciona los conocimientos teóricos y prácticos, fundamentales y necesarios para el diseño de una red LAN basada en las tecnologías mas conocidas y usadas en la actualidad, que darán al diseño de red el comportamiento deseado y optimo en las siguientes características de funcionalidad de red: un buena infraestructura como base para la prevención de problemas de capa física, el mejor desempeño, confiabilidad y la disponibilidad más alta. Con esto se logra reducir la presencia de fallas en el sistema de comunicaciones, además de tener un alto grado de respuesta para sobreponerse a las mismas debido a que se tendrán menos puntos latentes de posibles fallas.

La importancia de un buen cableado estructurado como principio base para una infraestructura confiable en términos de servicio, pone de manifiesto la necesidad de una instalación apegada a las normas mas actuales, esto dará una confiabilidad alta en la parte física de red. Se Considera que el primer punto de falla en cualquier diseño de red es la parte de infraestructura física, es por eso que se debe asegurar que el cableado y todo lo que concierne a este, sea instalado acorde a la normatividad existente en el ramo, con esto se logra contar con altos niveles de calidad en las instalaciones. Esta normatividad es mencionada en este trabajo. Los closets de telecomunicaciones deben estar totalmente acondicionados, el remate de los cables debe realizarse de manera correcta y respetando la disposición de los pares en el cable que se utilice de acuerdo a la norma, la identificación de cada uno de los elementos integrantes de la infraestructura para tener una mejor administración de los recursos, los equipos de comunicaciones deben ser tratados con sumo cuidado ya que estos se pueden dañar provocando una baja en su rendimiento, se deben respetar las distancias mínimas con respecto a otros servicios, se debe contar con un buen sistema de puesta a tierra implementado de manera correcta de acuerdo a la norma TIA/EIA 607.

Para respaldar un intercambio confiable de información en los canales de comunicación se debe tener en cuenta cada una de las características funcionales de los disposivitivos de interconexión de red o equipos de comunicaciones que se instalarán en la red LAN. De esta buena elección depende en gran medida el desempeño de la red LAN como un sistema integral, la correcta configuración de los mismos considerando que es lo que se va a implementar de manera lógica y saber en que capa del Modelo de Referencia OSI trabajarán, ayudaran a esto. Los niveles más bajos de colisiones en la red, ayudarán a mantener los canales libres al tráfico de información importante y de enrutamiento, el enrutamiento servirá para entregar de manera correcta los paquetes al host destino asegurando ninguna perdida de los mismos. En la actualidad existen switches que realizan funciones de enrutamiento, se deben considerar una buena elección para ser utilizados en la implementación de redes LAN como equipos terminales para la red WAN, ya que estos limitan los dominios de broadcast y las colisiones, mantienen anchos de banda bien definidos para cada unos de sus puertos y brindan enrutamiento hacia la WAN.

En la actualidad se ha logrado la integración de diversos servicios utilizando la infraestructura de la red LAN, con estos servicios de valor agregado se logra implementar una red multiservicios que brindará a los usuarios finales una gama amplia de posibilidades para su comunicación: ya sea interactiva y en tiempo real o bien con voz y video. Como ventajas importantes de mencionar se tiene las siguientes, el cliente tendrá un ahorro considerable en la implementación física, como ya se ha mencionado, estos servicios utilizan la misma infraestructura de red. En referencia a la VoIP, se tendrán

ahorros en las llamadas nacionales e internacionales, y las llamadas en el interior de la red serán gratuitas si el servidor de VoIP reside en el sitio.

La topología de red debe cumplir con los siguientes tres puntos de importancia: tiene que ser jerárquica, redundante y segura. Las funciones de cada capa deben estar bien definidas, el buen funcionamiento de cada una de ellas dará un alto grado de disponibilidad del servicio: se contará con un Backbone de alta velocidad y una capa de distribución constituida con buenos equipos de comunicaciones para que el acceso del usuario final no se vea afectado de ninguna forma. Una topología redundante aumentara el grado de disponibilidad de la red LAN, si se pierde el enlace hacia algún equipo de comunicaciones se podrá llegar al mismo por una ruta diferente. La seguridad en la red permitirá estar exento de ataques externos hacia la información, además de respaldar la información de las bases de datos, asegurando que no habrá pérdida de información.

Como parte importante para realizar un buen diseño de red se debe obtener la mejor caracterización de la red existente, esto si se da el caso, no restando importancia a ninguno de los puntos a considerar y que son plasmados en el capitulo 5, a partir de ellos se obtendrá una visión amplia de cuales podrían ser los nuevos requerimientos de algún cliente. Los nuevos requerimientos del cliente pueden haber sido causados por un crecimiento de usuarios en la red, la necesidad de nuevos servicios o aplicaciones, actualizar la red, etc. Estos nuevos requerimientos tienen que ser satisfechos en su totalidad, la topología de red y los equipos instalados serán acordes con estas nuevas características de diseño. En lo que respecta a la parte lógica y de configuración de red, se tiene que implementar un modelo de direccionamiento sencillo, práctico y de fácil comprensión para que posteriormente, ya cuando este funcionando la red, no se den problemas de enrutamiento o que algún paquete de información no llegue a su destino final. Para iniciar con una buena administración de red el primer paso es conjuntar y estructurar toda la información generada en el diseño de red, esta información tiene que ser plasmada en un documento de diseño, que será de gran utilidad para la administración. La red puede ser gestionada de manera remota, básicamente monitoreando el equipo terminal de red y el medio físico que brinda el enlace hacia la red WAN.

Implementar Calidad de Servicio (QoS) en la red LAN puede resultar una tarea más sencilla si se siguen las siguientes reglas: Utilizar exclusivamente switches o enrutadores basados en hardware. Los concentradores no pueden priorizar el tráfico, y los enrutadores basados en software pueden causar cuellos de botellas. Usar QoS como pretexto para no implementar el ancho de banda necesario. La configuración recomendada para la mayor parte de las redes es conmutación 10/100 Mbps en la conexión entre hosts y conexiones Gigabit Ethernet para los servidores y el Backbone. Asegurarse de que todos los dispositivos en la red pueden soportar calidad de servicio. La sola existencia de una parte del camino de los datos que no soporte QoS puede producir cuellos de botella y retardos, aunque globalmente se observen mejoras. Comprobar que todos los dispositivos con calidad de servicio son configurados de igual manera. De lo contrario, el mismo tráfico podría ser priorizado en unas secciones y no en otras. Conviene utilizar paquetes de gestión QoS global, capaces de configurar y checar todos los dispositivos simultáneamente. Clasificar el tráfico tan pronto como entre en la red. De no hacerlo hasta que llegue al Firewall o enrutador WAN, no se podrá garantizar prioridad de extremo a extremo. El lugar ideal para clasificar el tráfico es el switch en el closet de telecomunicaciones. Elegir switches y enrutadores basados en hardware que soporten tanto esquemas de marcación DSCP como 802.1p. Si en la red existen dispositivos que

sólo operen IEEE 802.1p, habrá que buscar switches capaces de efectuar conversiones entre esta técnica y DSCP. Asegurarse que los switches cuentan con más de una cola de tráfico por puerto, porque de lo contrario no podrán priorizar los datos. Para la mayoría de las aplicaciones, dos colas son suficientes y cuatro constituyen el ideal.

Por último, la gente que ya se encuentra operando una red LAN debe ser capaz de identificar y solucionar los problemas que se pueden presentar en la misma. Este trabajo puede ser de gran utilidad para ellos, ya que se da un enfoque general sin relacionarse con productos de algún fabricante en particular. De manera general, los problemas principalmente afectan la disponibilidad y desempeño de la red. Esos problemas deben ser solucionados de manera rápida y eficaz, esto se logra contando con buenas herramientas para la resolución de los mismos tanto en el aspecto físico, como en lo que respecta a la parte lógica. Se debe tener un monitoreo 7X24 de los equipos de comunicaciones para asegurar que los enlaces están “arriba” y que no se tiene ningún problema que afecte las características principales de funcionamiento de la red, esta tarea se vuelve mas sencilla si se utilizan aplicaciones para el monitoreo y administración de los recursos de la red. Es de suma importancia conocer cada uno de los pasos que se deben seguir para optimizar la resolución de problemas y así no entorpecer estos procedimientos. Diferenciar cada problema en particular ayudara a dar respuestas más rápidas a los problemas, y soluciones eficaces.

Glosario

2G: Red de telefonía móvil de segunda generación que utiliza sistemas digitales tipo GSM (*Global System for Mobile Communications*/Sistema Global de Comunicaciones Móvil) o CDMA (*Code Division Multiple Access*/Acceso Múltiple por División de Código).

2.5G: Red de telefonía móvil de segunda y media generación (transición entre sistemas 2G y 3G) que utiliza sistemas digitales tipo GPRS (*General Packet Radio Service*/Servicio General de Radio Paquetes), IS-95B o EDGE (*Enhanced Data for GSM Evolution*).

3G: Red de telefonía móvil de tercera generación que utiliza sistemas digitales con capacidad de gran ancho de banda. Este es el caso de UMTS (*Universal Mobile Telecommunications Service*/Servicio Universal de Telecomunicaciones Móviles) o CDMA-2000 (*Code Division Multiple Access*/Acceso Múltiple por División de Código).

ACK: *Acknowledgment*, Acuse de recibido de tramas de información.

ANSI: *American National Standards Institute*, Instituto Nacional Americano de Normalización. Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con normas, aprueban las normas nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de normalización. ANSI ayuda a desarrollar normas de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la Organización Internacional para la Normalización.

AP: *Access Point*, Punto de Acceso. Es el equipo de la red inalámbrica que se encarga de administrar las comunicaciones de todos los dispositivos que forman la red. El punto de acceso no sólo se utiliza para controlar las comunicaciones internas de la red. Sino que también hace de puente en las comunicaciones con las redes externas (redes cableadas e Internet).

ARP: *Address Resolution Protocol*, Protocolo de Resolución de Direcciones. Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826.

ARPANET: *Advanced Research Projects Agency Net*. Red de la Agencia de proyectos de Investigación Avanzada. Una red de conmutación de paquetes de gran importancia establecida en 1969. ARPANET fue desarrollada durante los años 70 por BBN y financiada por ARPA (y luego DARPA). Con el tiempo dio origen a la Internet. El término ARPANET se declaró oficialmente en desuso en 1990.

ATM: *Asynchronous Trasnfer Mode*, Modo de Transferencia Asíncrona. Norma internacional para el *relay* de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

Backbone. Parte de una red que actúa como camino primario para el tráfico que es generado de una red y destinado a otra red.

Backoff: Es un algoritmo que genera un periodo de tiempo aleatorio durante el cual se posterga el acceso al medio, con este proceso se evitan las colisiones.

Backplane. Es la conexión entre una interfase de procesador o tarjeta y el bus de datos, y da el poder de distribución dentro de buses de un chasis.

Balun**:** Su nombre proviene de la contracción de dos términos ingleses, «BALanced UNbalanced», es decir balanceado - no balanceado, Un *balun* convierte la impedancia desequilibrada de 75 ohms de un cable coaxial en la impedancia equilibrada de 120 ohms de un cable de par trenzado.

Bit. Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno.

Bluetooth: Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 metros). Al contrario de otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de hosts, sino, más bien, para comunicar un host o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su host, un host con su impresora, etc.

BPSK: *Binary Phase-Shift Keying*, Modulación Binaria por Salto de Fase.

BRAN: *Broadband Radio Access Network*, Red de Acceso Radio de Banda Ancha. Proyecto creado por ETSI al reconocer que HiperLAN/1 no era viable comercialmente.

Bridge: Puente. Dispositivo que conecta y transmite paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia OSI. En general, un puente filtra, envía o realiza un *flooding* de una trama entrante con base en la dirección MAC de esa trama.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast.

BSS: *Basic Service Set*, Conjunto de Servicios Básicos. Es una de las modalidades de comunicación en las que se pueden configurar los hosts de una red inalámbrica. En este caso, la red inalámbrica dispone de un equipo (punto de acceso) que se encarga de administrar las comunicaciones (internas o externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo de infraestructura.

Buffer: Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

Bus. Camino de la señal física integrado por los alambres u otros medios a través de los cuales las señales se pueden enviar a partir de un host a otro. A veces llamado *highway*.

BWA: *Broadband Wireless Access*, Acceso Inalámbrico de Banda Ancha. Es un acrónimo con el que se hace referencia al acceso inalámbrico de banda ancha.

Byte: Serie de 8 dígitos binarios consecutivos que operan como una unidad.

Cable UTP. *Unshielded Twisted Pair*. Medio de cuatro pares de alambre de cobre, usados en una variedad de redes. Cinco tipos de cable UTP son comúnmente usados: categoría 1, categoría 2, categoría 3, categoría 4 y categoría 5. Sin embargo, últimamente han entrado al mercado otras categorías como 5e, 6 y 7.

Campus: Conjunto de terrenos e instalaciones universitarias.

Carrier: Portadora. Señal de frecuencia fija generalmente, que es modulada por la señal de información a fin de transportarla.

CCA: *Clear Channel Assessment*, Valoración de la Disponibilidad del Canal.

CCK: *Complementary Code Keying*, Modulación de Código Complementario.

Centro de Cómputo. Lugar acondicionado para alojar servidores y equipos de comunicaciones.

CIDR *Clasless Inter.-Domain Routinrg*, Enrutamiento sin Clase entre Dominios**:** Técnica reconocida por BGP y basada en el agregado de rutas. CIDR permite que los enrutadores agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los enrutadores principales. Con CIDR, un conjunto de redes IP aparece ante las redes ajenas al grupo como una entidad única de mayor tamaño.

Circuito Virtual: Circuito creado para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par VPI/VCI y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se usan en Frame Relay y X.25. En ATM, un circuito virtual se denomina canal virtual. A veces se abrevia VC.

Closet de comunicaciones. Es el cuarto donde llega todo el cableado estructurado y se encuentran equipos de comunicaciones (Enrutadores, Switches, etc).

Concentrador: *Hub*. En general, es un dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto.

Cookie Cutter. Consiste en ahorrar problemas a los administradores de la red, mientras también reduce la vulnerabilidad de errores de la configuración.

CRC: *Cyclic Redundancy Check*, Comprobación Cíclica de Redundancia. Son unos datos adicionales que se adjuntan al final de la información para poder comprobar fácilmente que no ha habido errores en la transmisión. Los datos CRC son el resultado de hacer determinadas operaciones matemáticas con la información original. Como las operaciones son las mismas en origen y en destino, si el resultado no es el mismo, es que hay error en la transmisión.

CSMA/CA: *Carrier Sense Multiple Access/Collision Avoidance*, Acceso Múltiple por Detección de Portadora con Evitación de Colisión. Es el sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión).

CSMA/CD, *Carrier Sense Multiple Access/Collision Detection*, Acceso múltiple con Detección de Portadora con Detección de Colisiones. Mecanismo de acceso a medios

dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

CTS: *Clear to Send*, Listo para Enviar.

CW: *Contention Window*, Ventana de Contienda. CW es un número entero dentro del rango de valores de las características físicas $CW_{mín} \leq CW \leq CW_{máx}$.

DARPA: *Defense Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzada. Agencia gubernamental de los EE.UU. que financió la investigación y la experimentación con la Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994.

Datagrama IP: Paquete IP. Unidad fundamental de información transmitida a través de la Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación del encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

dB: Decibel. Relación entre dos parámetros utilizando logaritmos de base 10. Se utiliza debido a que facilita los cálculos cuando intervienen cantidades muy grandes y muy pequeñas.

dBi: Decibeles referidos a la potencia radiada por una antena isotrópica.

DBPSK: *Differential Binary Phase-Shift Keying*, Modulación Diferencial Binaria por Salto de Fase.

DCF: *Distributed Coordination Function*, Función de Coordinación Distribuida. Facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etc.) entre todos los hosts de la red.

DIFS: *DCF Interframe Space*. Usado por hosts operando bajo la función DCF para transmitir tramas de datos.

Dirección de Broadcast: Dirección especial reservada para enviar un mensaje para todas los hosts.

Dirección de Multicast: Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo.

Dirección de Unicast: Dirección que especifica un solo dispositivo de red.

Dirección MAC: Es un número único que asignan los fabricantes a los dispositivos de red (adaptadores de red y puntos de acceso). Este número es permanente y viene grabado en el propio dispositivo para permitir identificarlo de forma inequívoca. Las direcciones

MAC están formadas por 12 caracteres alfanuméricos (en sistema numérico hexadecimal), por ejemplo, 12-AB-56-78-90-FE.

DNS. *Domain Name Server*. Sistema usado en Internet para traducir direcciones en nombres de nodos de red.

DoD: *Department of Defense*, Departamento de Defensa. Organización gubernamental de los EE.UU. responsable por la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

Dominio de Broadcast: Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto. Los dominios de broadcast normalmente se encuentran limitados por enrutadores porque los enrutadores no envían tramas de broadcast.

DQPSK: *Differential Quadrature Phase Shift Keying*, Modulación Diferencial de Cuadratura por Salto de Fase.

DS: *Distribution System*, Sistema de Distribución. Sistema usado para interconectar BSSs e integrar redes de área local inalámbricas para crear una ESS.

DSSS: *Direct Sequence Spread Spectrum*, Espectro Expandido por Secuencia Directa. Es la técnica de modulación utilizada por los sistemas IEEE 802.11b (Wi-Fi) para transmitir datos a alta velocidad (11 Mbps).

DVMRP: *Distance Vector Multicast Routing Protocol*, Protocolo de Enrutamiento Multicast por vector de Distancia. Es un protocolo usado para propagar tablas de enrutamiento vía multicast.

Encabezado: *Header*. Información de control colocada antes de los datos al encapsularlos para la transmisión en red.

E3**.** Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 34,368 Mbps. Las líneas E3 pueden ser dedicadas para el uso privado de carriers comunes.

EIFS: *Extended Interframe Space*. El EIFS está definido para proveer suficiente tiempo para otro host para reconocer que fue, para este host, una incorrecta recepción de la trama antes de que este host comience la transmisión.

EMI. Fuentes de interferencia magnética. Interferencia por señales electromagnéticas que puede causar una reducción en la integridad de datos e incremento en la tasa de errores en el canal de transmisión.

Enrutador: *Router*. Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los enrutadores envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Enrutamiento: *Routing*. Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

ESS: *Extended Service Set*. Conjunto de Servicios Extendido. Es una de las modalidades en las que se puede configurar una red local inalámbrica Wi-Fi. Reciben este nombre las redes inalámbricas que están formadas por más de un punto de acceso.

Estación de trabajo. Un sistema de computación de alto rendimiento para un usuario.

Ethernet: El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 Mbps, 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

ETSI: *European Telecommunications Standards Institute*. Instituto Europeo de Normas de Telecomunicaciones. Creado en marzo de 1989 y con sede en Sophia-Antipolis, cerca de Niza.

Failover. Redundancia para sobreponerse a fallas.

FDDI. *Fiber Distribution Digital Interface*: especificación para la red de datos con token passing, usando óptica, con una tasa de 100 Mbps, con distancias arriba de 2 km. Definida por el ANSI X3T9.5. FDDI usa una arquitectura para proveer redundancia.

FHSS: *Frequency Hopping Spread Spectrum*, Espectro Expandido por Salto de Frecuencia. Es una técnica de modulación utilizada tanto por los sistemas IEEE 802.11 como Bluetooth. Transmite datos a baja (1 Mbps) por lo que en la versión 802.11b se sustituyó por el sistema DSSS para poder transmitir datos a alta velocidad (11 Mbps).

Firmware: Es un código de programa que se graba en las unidades de hardware de los equipos. A través del firmware los fabricantes consiguen actualizar el hardware sin cambiar el chip. Estos códigos se guardan en unos chips de memoria conocidos como PROM. Estos chips tienen la particularidad de que no se borran cuando no tienen alimentación eléctrica y pueden ser programados.

Forwarding. Proceso de envío de tramas a través de dispositivos de interconexión.

Fragmentar: Proceso de dividir un paquete en unidades más pequeñas al transmitir a través de un medio de red que no puede acomodar el tamaño original del paquete.

Gateway: Puerta de Enlace. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. El gateway adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente para interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta. En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término enrutador se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro.

GFSK: *Gaussian Frequency-Shift Keying*, Modulación Gausiana por Salto de Frecuencia.

Granja de Servidores. Área donde se localizan servidores locales o servidores externos.

Half-Duplex: Semiduplex. Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora.

Header: ·Encabezado. Parte inicial de un paquete de datos a transmitir, que contiene la información sobre los puntos de origen y de destino de un envío y sobre el control de errores.

HiperLAN: *High-Performance Radio Local Area Network*, Red de Área Local de Radio de Alto Rendimiento. Es una norma de red de área local inalámbrica definido por ETSI que permite transmitir datos hasta 54 Mbps trabajando en la banda de 5 GHz.

HiperLAN/1: Primera versión de la norma HiperLAN, publicada en 1996, trabajaba en la banda de frecuencias de 5 GHz y alcanzaba velocidades de hasta 54 Mbps.

HiperLAN/2: Segunda versión de la norma HiperLAN. Esta norma es el resultado de un proyecto llamado BRAN. HiperLAN/2 está diseñado para ofrecer accesos inalámbricos de alta velocidad a redes ATM, a redes celulares de tercera generación, Fireware IEEE 1394 y redes IP. HiperLAN/2 ofrece velocidades de transmisión de 54 Mbps utilizando el sistema OFDM. Las frecuencias utilizadas son 5.25 GHz a 5.35 GHz para sistemas de interior a 200 mW de potencia y de 5.47 GHz a 5.725 GHz para sistemas de exterior a 1000 mW de potencia.

HomeRF: *Home Radio Frequency*, Radio Frecuencia del Hogar. Es una tecnología de red de área local inalámbrica que en su día fue promovida por Intel (además de otros). Existen tres versiones en el mercado que alcanzan los 1, 6, 10 y 40 Mbps, respectivamente. En cualquier caso, HomeRF ha quedado hoy día en el olvido debido al auge de Wi-Fi.

Hardware: Componentes físicos de una computadora o dispositivo informático, incluyendo el procesador, memoria, dispositivos de E/S y discos.

Host. Es cualquier computadora o dispositivo conectado a una red TCP/IP. Computadora en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y enrutadores.

IBSS: *Independent Basic Service Set*, Conjunto de Servicios Básicos Independientes. Es una de las modalidades de comunicación en las que se pueden configurar los hosts de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre los distintos hosts que forman la red. Este modo de conexión también es conocido como modo ad hoc, modo independiente o peer to peer (igual a igual).

ICMP: *Internet Control Message Protocol*, Protocolo de Mensajes de Control en Internet**:** Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP. Documentado en RFC 792.

IDF. Sala de comunicaciones secundaria para un edificio donde funciona una topología de networking en estrella. El IDF depende del MDF.

IEEE: *The Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos. Es una asociación mundial de ingenieros de este sector. El IEEE forma también el comité de normalización que recomienda al ANSI sobre las normas de tecnologías de redes de área local.

IMS: *Industrial, Scientific and Medecine*, Industrial, Científica y Médica. Estas siglas hacen referencia a la banda de frecuencias radioeléctricas reservadas a aplicaciones de este tipo. Ésta es la banda de frecuencias en las que actúa Wi-Fi.

Interfaz: 1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

Internet: La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general Internet.

Internetwork: Industria dedicada a la conexión de redes entre sí. Este término se refiere a productos, procedimientos y tecnologías.

IP: *Internet Protocol*, Protocolo de Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo.

IPX: Intercambio de Paquetes de Internetwork. Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo. IPX es similar a IP y XNS.

IrDA: *Infrared Data Association*. Es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene dos normas: IrDA-Control e IrDA-Data.

IrDA-Control: Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos.

IrDA-Data: Es un protocolo orientado a crear redes de datos de corto alcance.

ISO: *International Standard Organization*, Organización Internacional para la Normalización. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OSI, utilizado por las redes públicas de conmutación de paquetes.

Jitter. Se denomina así a la medida de variación de retraso entre paquetes consecutivos para un determinado flujo de tráfico. Posee un efecto pronunciado en aplicaciones sensibles al retraso en tiempo real, como voz y video. Estas aplicaciones están preparadas para recibir paquetes en un ritmo periódico constante y un retraso fijo entre paquetes consecutivos. Como el ritmo de llegada varía, el jitter incide sobre la velocidad de la aplicación. Una cantidad mínima de jitter puede ser aceptable, pero a medida que el jitter aumenta, la aplicación se torna inútil. Algunas aplicaciones (como telefonía IP) pueden compensar pequeños niveles de jitter. Como la aplicación de voz requiere audio para poder desarrollar un ritmo constante, si el siguiente paquete no llega dentro del tiempo de reproducción, la aplicación puede repetir el paquete de voz previo hasta que el próximo paquete de voz llegue. Sin embargo, si el siguiente paquete también se demora demasiado, directamente es descartado cuando llega, dando como resultado una pequeña suma de audio distorsionado. Todas las redes tienen un poco de jitter, debido a la variabilidad del retraso introducido por cada nodo de red cuando los paquetes están en tiempo de espera. Sin embargo, al controlarse el jitter, el QoS puede ser conservado.

LAN. *Local Area Network,* es una red de alta velocidad, conectividad que provee tolerancia a fallas de la red de datos a un grupo de computadoras, impresoras, y otros dispositivos en proximidad cercana el uno al otro, por ejemplo, adentro un edificio de oficinas, una escuela o un hogar. Las LANs ofrecen muchas ventajas a los usuarios conectados, incluyendo acceso compartido para dispositivos y aplicaciones, intercambio de archivos entre usuarios conectados, y comunicación entre usuarios vía correo electrónico y otras aplicaciones.

LLC: *Logical Link Control*, Control de Enlace Lógico. La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión.

LMDS: *Local Multipoint Distribution Service*, Servicio Local de Distribución Multipunto. Es una tecnología inalámbrica vía microondas para comunicación entre puntos fijos. Esto quiere decir que no es una tecnología pensada para ser utilizada por terminales en movimiento. El rango de frecuencias utilizado varía entre 2 y 40 GHz dependiendo de la regulación del país en el que se utilice.

MAC: *Medium Access Control*, Control de Acceso al Medio. Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

MAN: *Metropolitan Area Network*, Red de Área Metropolitana. Es un acrónimo con el que se hace referencia a las redes de área metropolitana.

Máscara de Subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Mbps: MegaBits por Segundo. Es una unidad de medida de la velocidad de transferencia de datos. Un Megabit por segundo significa que se transfieren 1,048,576 (1,024 x 1,024) bits cada segundo. Un bit es la unidad más pequeña de información (un 0 ó un 1).

MDF. Sala de comunicaciones principal donde se concentran las conexiones de los IDFs.

MIB: *Management Information Base*, Base de Datos de la Información de Gestión.

MLME: *MAC Layer Management Entity*, Entidad de Gestión de la Capa MAC.

MMDS: *Multichannel Multipoint Distribution Service*, Servicio Multicanal de Distribución Multipunto.

MPDU: *MAC Protocol Data Unit*, Unidad de Datos del Protocolo MAC.

MTU *Maximum Transmission Unit*, Unidad Máxima de Transmisión. Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

MSDU: *MAC Service Data Unit*, Unidad de Datos del Servicio MAC.

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

NAT. *Network Address Translation*. Mecanismo para reducir la necesidad de direcciones IP globales únicas (homologadas). El NAT permite una organización con las direcciones no globales únicas (privadas) para conectar a Internet traduciendo esas direcciones en espacio de direcciones globales ebrutables en Internet.

NAV: *Network Allocation Vector*, Vector de Asignación de Red.

NetWare. Popular sistema operativo de red distribuido desarrollado por Novell. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos.

Networking: Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

Número de Saltos: Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino.

Octeto: 8 bits. En networking, el término octeto se utiliza a menudo (en lugar de byte) porque algunas arquitecturas de máquina utilizan bytes que no son de 8 bits de largo.

OFDM: *Orthogonal Frequency Division Multiplexing*, Multiplexación Ortogonal por División en Frecuencia. Es una técnica de modulación utilizada por las redes de área local inalámbrica de alta velocidad (IEEE 802.11a y HiperLAN2). Permite transmitir datos de hasta 54 Mbps.

Orientado a Conexión: Transferencia de datos que requiere que se establezca un circuito virtual.

OSI: *Open Systems Interconnect*, Interconexión de Sistemas Abiertas. Se trata de una serie de protocolos normalizados por la Organización Internacional para la Normalización, ISO.

OUI: *Organizationally Unique Identifier*, Identificador Exclusivo de Organización**:** Tres octetos asignados por el IEEE en un bloque de direcciones de LAN de 48 bits.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

PCF: *Point Coordination Function*, Función de Coordinación de Punto. Facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial evitando las demoras.

PCMCIA: *Personal Computer Memory Card International Association*, Asociación Internacional de Tarjetas de Memoria para Computadoras Personales. Se trata de una asociación de fabricantes de equipos que en 1989 sacó al mercado un tipo de puerto y dispositivo de pequeño tamaño que permite que se le pueda instalar todo tipo de periféricos a las computadoras personales. En un principio se dedicaron sólo a ampliar la memoria, de ahí su nombre.

PDM: *Physical Medium Dependent*, Dependiente del Medio Físico. PDM es la que se encarga de la difusión de la señal.

PHY: *Physical Layer*, Capa Física. Es la capa que se ocupa de definir los métodos por los que se difunde la señal.

PIFS: *PCF Interframe Space*. Usado por hosts operando bajo la función PCF para ganar prioridad de acceso al medio sobre los demás host.

PLCP: *Physical Layer Convergence Procedure*, Procedimiento de Convergencia de la Capa Física. PLCP se encarga de convertir los datos a un formato compatible con el medio físico.

PLME: *PHY Layer Management Entity*, Entidad de Gestión de la Capa Física.

Portal: Componente lógico usado para integrar arquitecturas IEEE 802.11 y LANs tradicionales.

PPM: *Pulse Position Modulation*, Modulación por Posición de Pulso.

PROM: *Programmable Memory of Only Reading*, Memoria Programable de Sólo Lectura. ROM que puede programarse utilizando equipo especial. Las PROM pueden ser programadas solamente una vez.

Protocolo: Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Proxy: Entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad.

QAM: *Quadrature Amplitude Modulation*, Modulación de Amplitud en Cuadratura.

QoS: *Quality of Service*, Calidad de Servicio. Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

QPSK: *Quadrature Phase-Shift Keying*, Modulación por Salto de Fase en Cuadratura.

Reensamblaje: Colocación en su formato original de un datagrama IP en el destino después de su fragmentación en el origen o en un nodo intermedio.

Rendimiento: Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

RFC: *Request For Comment*, Petición para Comentar. Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

Roaming: Se conoce por este nombre a la posibilidad que tienen los equipos inalámbricos de desplazarse dentro del área de cobertura de una red inalámbrica sin perder la conexión.

RTS: *Request to Send*, Solicitud para Enviar.

SIFS: *Short Interframe Space*. Se usa para separar transmisiones de una misma conexión (una trama ACK, una trama CTS, etc).

SMTP. *Simple Mail Transfer Protocol*. Protocolo de Internet que proporciona servicios de correo electrónico.

Software: Colección de instrucciones electrónicas escritas por programadores, usando un lenguaje de programación que la CPU de un host puede interpretar para llevar a cabo una tarea especifica; generalmente se guarda en almacenamiento magnético; también llamado programa de computadora o programa.

Spread Spectrum: Espectro Expandido o Espectro Disperso. Es un sistema de difusión de las señales radioeléctricas. Este sistema utiliza un ancho de banda mayor al estrictamente necesario a cambio de conseguir reducir la vulnerabilidad a las interferencias y garantizar la coexistencia con otras transmisiones.

Strictly-Ordered: Estrictamente Ordenado.

Subred: 1. Red segmentada en una serie de redes más pequeñas. 2. En redes IP, una red que comparte una dirección de subred individual. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina subnetwork. 3. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo exclusivo y que utiliza un protocolo de acceso de red exclusivo.

Switch: Conmutador. Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches de LAN envían tráfico basándose en las direcciones MAC. Los switches de LAN a menudo se clasifican según el método utilizado para enviar tráfico: conmutación de paquetes por método de corte o conmutación de paquetes por almacenamiento y envío.

T3**.** Servicio de portadora WAN digital que transmite datos formateados DS-3 a 44,736 Mbps a través de la red de conmutación telefónica.

TCP/IP: *Transmission Control Protocol/Internet Protocol*, Protocolo de Control de Transmisión/Protocolo de Internet. Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años ’70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

TKIP: *Temporal Key Integrity Protocol*, Protocolo de Integridad de Clave Temporal. Este sistema asegura la confidencialidad de los datos. Es una mejora en el cifrado de datos y una ventaja que aportan las especificaciones de WPA.

Token Ring: LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo.

Tormenta de Broadcast: Suceso de red no deseado, en el que se envían varios broadcasts simultáneamente a todos los segmentos de red. Una tormenta de broadcast usa una parte considerable del ancho de banda de la red y normalmente hace que se agoten los tiempos de espera de la red.

Trama: *Frame* o Datagrama. Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

UTP: Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hasta hoy, hay ocho tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5, cableado de Categoría 6, cableado de Categoría 7 y cableado de Categoría 8.

Vertical. Lugar por donde pasan las escalerillas y tubería que lleva el cable UTP, Fibra o de corriente eléctrica de los pisos de un Edificio.

VLAN. *Virtual LAN*. Grupo de dispositivos en una o más LANs que son configuradas (usando software de administración) de modo que ellas pueden comunicarse como si estuvieran agregadas en la misma red, cuando de hecho éstas están localizadas en segmentos diferentes. Porque las VLANs se basan su funcionamiento en conexiones lógicas en vez de conexiones físicas, y son extremadamente flexibles.

WDS: *Wireless Distribution System*, Sistema de Distribución Inalámbrica.

WECA: *Wireless Ethernet Compatibility Alliance*, Alianza de Compatibilidad Ethernet Inalámbrica. Es una asociación de fabricantes de equipos de red creada en 1999 con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos. WECA es la creadora de la marca Wi-Fi y es quien certifica los equipos con esta marca.

WEP: *Wireless Equivalency Protocol*, Protocolo de Equivalencia con Red Cableada. Es el sistema de cifrado de datos que incorporan las redes inalámbricas, definidas en la norma IEEE 802.11.

Wi-Fi: *Wireless Fidelity*, Fidelidad Inalámbrica. Es una marca creada por la asociación WECA con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos.

WAN. *Wide Area Network*, es una red de comunicaciones de datos, atravesando a lo largo de una área geográfica, como un estado, provincia o país, y utiliza a menudo la infraestructura de transmisión proporcionada por los carriers comunes, como compañías telefónicas.

WLAN. *Wireless Local Area Network*, Red de Área Local Inalámbrica. Es un acrónimo con el que se hace referencia a las redes de área local inalámbricas.

WMAN: *Wireless Metropolitan Area Network*, Red Inalámbrica de Área Metropolitana. Es un acrónimo con el que se hace referencia a las redes de área metropolitana inalámbricas.

WPA: *Wi-Fi Protected Access*, Acceso Wi-Fi Protegido. Son unas especificaciones de seguridad basadas en la norma IEEE 802.11i que incrementa fuertemente el nivel de protección de datos y de control de acceso a las redes Wi-Fi. Las facilidades de seguridad ofrecidas por WPA pueden implantarse en las redes Wi-Fi existentes mediante una instalación de softaware.

WPAN: *Wireless Personal Area Network*, Red Inalámbrica de Área Personal. Este tipo de redes cubren distancias inferiores a 10 metros. Estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario (por ejemplo, una computadora con la impresora). Éste es el caso de la tecnología Bluetooth o de IEEE 802.15.

Bibliografía

- Interconnecting Cisco Network Devices. Cisco. Volumen 1. Versión 1.1. 2000. USA.
- Designing Cisco Networks. Volume 1, Version 2.0, 1999, Cisco Systems.
- Recomendación X.200 ITU-T (CCITT)
- Traffic Analysis and Network Health Report
- Deploying H.323 Applications in Cisco Networks, Sam Kotha, Cisco Systems, Inc.
- Virtual LANs and 802.1Q, Marconi Communications. November 2000.
- Gigabit Ethernet en fibra y Cobre, Soluciones de Red Gigabit de Cisco Systems e Intel, Copyright © 2001 Intel Corporation and Cisco Systems, Inc. Reservados todos los derechos.
- Voice and Data Integration White Paper, Introduction to Voice over Local Area Networks, Anixter.
- Voice over internet Protocol, Anixter.
- Cisco Lan Switching, CCIE Profesional Development, 1999, Cisco Systems.
- Cisco Internetwork Design. Volume 1, Version 3, 1999, Cisco Systems.
- Wi-Fi. Cómo construir una red inalámbrica. José A. Carballar. Ed. Alfaomega. 2004.
- ANSI/IEEE Std 802.11, 1999 Edition.
- IEEE Std 802.11b, 1999 Edition. (Supplement to IEEE Std 802.11-1999).
- IEEE Std 802.11a, 1999 Edition. (Supplement to IEEE Std 802.11-1999).
- IEEE Std 802.11g, 2003 Edition. (Amendment to IEEE Std 802.11 , 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)
- Top-Down Network Design, Priscilla Oppenheimer, Cisco Press, 1999.
- Norma IEEE 802.1D Media Access Control (MAC) Bridges
- Norma IEEE 802.1Q Virtual Bridged Local Area Networks
- Capítulo 2: Conmutación LAN, CCNA-CNAP, Cisco.

Referencias Electrónicas

- http://www.um.es/~gtiweb/fjmm/ttsite-plan2/modelos.htm#5-1
- http://www.cse.ohio-state.edu/~jain/cis788-97/ftp/virtual_lans/index.htm
- http://nodo.uagrm.edu.bo/inf050.uagrm.edu.bo/2002/n/gn03/ModeloOsi%5COsi.html#osi
- http://ingenet.ulpgc.es/~ablesa/telecom/optimizaredes/routing5.htm
- http://www.optimized.com/COMPENDI/
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm
- http://members.tripod.com/hgr/redes.html
- http://www.pchardware.org/redes/redes_ethernet.php
- http://www.lcc.uma.es/~eat/services/proto802/csmacd.html
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm
- http://www.cybercursos.net/cursos-online/fast-ethernet/fastethernet.htm
- http://lwww.gigabitsolution.com
- http://lwww.10gea.org
- http://standards.ieee.org/catalog/IEEE802.3.html
- http://lgrouper.ieee.org/groups/802/3/index.html
- http://mailweb.udlap.mx/~tesis/lis/perez_p_jg/capitulo2.html
- http://www.tst.es/streaming3.htm
- http://www.cnice.mecd.es/tecnologica/experto/interconexion/
- http://www.noticias3d.com/articulos/200206/hubswitch/1.asp
- http://nodo.uagrm.edu.bo/inf050.uagrm.edu.bo/2002/m/gm14/Disp_interconexion.htm
- http://www.wi-fi.com
- http://www.htmlweb.net/linux/redes/redes_linux_12.html
- http://consultasccna.com/

- http://www.rfc-es.org/rfc/rfc1918-es.txt
- http://www.windowstimag.com/atrasados/1998/24_oct98/articulos/dhcp1.htm
- http://student.bii.a-star.edu.sg/~danielc/Network_Layers/layer01.htm
- http://www.mcmtelecom.com.mx/news/ancho_de_banda.html
- http://www.tml.hut.fi/Opinnot/Tik10.551/1999/papers/08IEEE802.1QosInMAC/qos.html
- http://qos.iespana.es/qos/CAPITULO8.htm
- http://www.ascenetworks.com/support/faq.htm
- http://www.javvin.com/protocol8021P.html
- http://www.eveliux.com/telecom/cpswitching.html
- http://mailweb.udlap.mx/~tesis/lis/perez_p_jg/capitulo2.html
- http://www.tst.es/streaming3.htm