VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"Diseño e Implementación de la Red Inalámbrica para el Laboratorio de Dispositivos Lógicos Programables"

T E S I S

Como requisito para obtener el título de

Ingeniero en Computación

P r e s e n t a:
Yenni Trejo Zamora

DIRECTOR DE TESIS:

ING. NORMA ELVA CHÁVEZ RODRÍGUEZ

CIUDAD UNIVERSITARIA, MÉXICO, D. F. JUNIO 2005

Para mis padres y para una persona que compartió y comparte conmigo su sentido del tiempo mágico.

AGRADECIMIENTOS:

Se cierra un ciclo de mi vida y empiezan nuevos. Agradezco a todas aquellas personas que compartieron conmigo su tiempo en esta Universidad, mis maestros, mis compañeros, mis amigos y todos aquellos que hicieron realidad esta meta cumplida.

Un agradecimiento especial a mis padres: gracias por darme la oportunidad de brindarme el estudio, de enseñarme que todo aquello que vale la pena merece un esfuerzo, de enseñarme que teniendo responsabilidad en todo lo que hacemos nos abrirá las puertas y hasta el momento así ha sido.

Agradezco a mi maestra y tutora por el apoyo, el tiempo y la dedicación que me presto para verse finalizado este proyecto y por todo aquello que me enseño con sabiduría en clase, que hasta el momento he aplicado en el trabajo.

Y por último y no porque sea menos importante, agradezco a Juan Orosco la ayuda, el tiempo y la guía que me dio durante todo este tiempo que duró la tesis. Espero que siempre este a mi lado para compartir y disfrutar mis triunfos.

Diseño e Implementación de una red inalámbrica para el Laboratorio de Dispositivos Lógicos Programables.

I N D I C E

CAPITULO 3. **Protocolos de control de acceso al medio y Estándares de redes**

INTRODUCCIÓN

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadoras), así como a la puesta en orbita de los satélites de comunicación.
A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.
La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

Las redes de comunicación personal inalámbricas basadas en las nuevas tecnologías digitales han surgido como un importante campo de la actividad de las telecomunicaciones. Esto es principalmente debido al éxito de teléfonos móviles, Notebook, etc. Los días se acercan rápidamente en los cuales podremos enviar y recibir e-mail o facsímiles, ver y hablar al mismo tiempo, desde cualquier lugar usando a un pequeño aparato manual o simplemente con una computadora portátil.

A principios del siglo 20, la distinción en comunicación, entre la telefonía y computación desaparecieron y ha llegado la transmisión integrada de la información en varios medios de comunicación (voz, datos, imagen, y texto).

Debido a los avances recientes en fibra, las redes inalámbricas de la próxima generación deben diseñarse para encajar fácilmente y coexistir con la red ISDN (Integrated Services Digital Network), con el fin de evitar una desigualdad seria entre las redes alambricas e inalámbricas (por llamarles de alguna manera).

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.
Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.
Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivo compartido.
Este objetivo conduce al concepto de redes con varios ordenadores en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.
Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo mas procesadores. Con máquinas grandes, cuando el sistema esta lleno, deberá reemplazarse con uno mas grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.
Otro objetivo del establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si. Con el ejemplo de una red es relativamente

fácil para dos o más personas que viven en lugares separados, escribir informes juntos. Cuando un autor hace un cambio inmediato, en lugar de esperar varios días para recibirlos por carta. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podrían mejorarse la fiabilidad y el rendimiento. Sin embargo, la disponibilidad de una WAN (ya estaba antes) si genera nuevas aplicaciones viables, y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Para dar una idea sobre algunos de los usos importantes de redes de ordenadores, veremos ahora brevemente tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido. Una compañía que ha producido un modelo que simula la economía mundial puede permitir que sus clientes se conecten usando la red y corran el programa para ver como pueden afectar a sus negocios las diferentes proyecciones de inflación, de tasas de interés y de fluctuaciones de tipos de cambio. Con frecuencia se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se está ajustando constantemente ó necesita de una máquina muy grande para correrlo.

Todas estas aplicaciones operan sobre redes por razones económicas: el llamar a un ordenador remoto mediante una red resulta mas económico que hacerlo directamente. La posibilidad de tener un precio mas bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuado se están transmitiendo los datos.
Una tercera forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (INTERNET). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

Hoy en día, los sistemas educacionales de todo el mundo están teniendo dificultades para seguir la rápida evolución de la Tecnología de la Información. Aún en las grandes naciones desarrolladas, muchas salas de clases carecen de conexiones a la Internet, dejando a los estudiantes mal preparados para las oportunidades y trabajos generados por la economía de la información. En el caso de aquellas instituciones educacionales que sí cuentan con computadores y acceso a Internet, a menudo deben esforzarse para mantener e incrementar sus recursos de información.

En la actualidad, el laboratorio de Dispositivos Lógicos Programables tiene grandes limitaciones generando retrasos en los proyectos de los estudiantes y por ende un alto índice de reprobación. Esta propuesta de tesis tiene como finalidad dar respuesta a estos retos en beneficio de cientos de miles de estudiantes pertenecientes a la Facultad de Ingeniería.

OBJETIVOS

OBJETIVO GENERAL

Diseñar un sistema de red inalámbrica que permita la fácil transferencia de archivos como apoyo al aprendizaje de algunas asignaturas impartidas en la Facultad de Ingeniería.

OBJETIVOS PARTICULARES

- Cubrir las necesidades y objetivos del Laboratorio de Dispositivos Lógicos Programables.
- Ampliar los conocimientos sobre equipos de red que existen actualmente en el mercado
- Seleccionar la tecnología y arquitectura de red de cómputo adecuada.

ANTECEDENTES.

1.1. Breve reseña histórica

El desarrollo del hombre desde el nivel físico de su evolución, pasando por su crecimiento en las áreas sociales y científicas hasta llegar a la era moderna se ha visto apoyado por herramientas que extendieron su funcionalidad y poder como ser viviente.

Durante la época prehistórica, el hombre se valió de la piedra, la madera y el metal para construir extensiones de su cuerpo: Un martillo o punta de lanza de piedra, obsidiana, madera endurecida al fuego para tener un alcance mayor de sus brazos y dominar a las bestias para conseguir el sustento diario.

Después domesticó a los animales y construyó artefactos cada vez más complejos: Un arco para enviar sus "brazos" (flechas) en la distancia y subyugar a animales más peligrosos. Y así como extendió sus brazos, pronto encontró la forma de extender sus piernas para alcanzar lugares más lejanos: fabricó navíos para cruzar ríos, lagos y mares; carretas que los llevaban a lugares distantes más rápido que sus pies y con cargas mayores y hasta refinó las artes que le permitieron tener en el hogar paisajes y monumentos de la naturaleza para darse la sensación de tenerlos a su alcance en todo momento.

Finalmente, y sintiéndose conciente de su habilidad creativa, metódicamente elaboró procedimientos para organizar su conocimiento, sus recursos y manipular su entorno para su comodidad, impulsando las ciencias y mejorando su nivel de vida a costa de sacrificar el desarrollo natural de su ambiente, produciendo así todos los adelantos a los que un gran sector de la población conocemos: automóviles, aeroplanos, trasatlánticos, teléfonos, computadoras, televisiones, etc.

En el transcurso de todo este desarrollo, lo que nos interesa revisar es la evolución de un sector tecnológico: El cómputo electrónico. Este nació con las primeras computadoras en la década de los 40's con los tubos al vacío y los tableros de control enchufables. Y fue así porque la necesidad del momento era extender la rapidez del cerebro humano para realizar de algunos cálculos aritméticos y procedimientos repetitivos.

Las redes de datos.

Una vez resuelto el problema de extender el poder de cálculo del cerebro humano nació o se comenzó a atacar el problema de compartir los datos y la información que ese poder de cálculo produjo, lo cual nos llevó a inventar la forma de compartir recursos (impresoras, graficadores, archivos, etc) a través de algún medio de transmisión usando una serie de reglas (protocolos) para accesar y manipular dichos recursos.

Los sistemas distribuidos.

Las redes de computadoras nos permitieron reunir esfuerzos aislados en esfuerzos conjuntos que producían bienes mayores (sinergia). Sin embargo, en una red la forma de accesar a dichos recursos va de la mano con conocer la manera de llegar a esos recursos y saber cómo manipularlos, es decir, no hay transparencia. El siguiente salto tecnológico-filosófico es extender las redes de cómputo hacia los sistemas distribuidos (una entidad vista como un todo y conformado por múltiples cerebros ubicados en localidades alejadas unas de otras que nos ofrecen servicios y recursos sin importar su ubicación). Esos recursos deben estar disponibles en el momento adecuado y que los datos o información que produzcan sean altamente confiables, esto es, que no sufran deterioro durante su transmisión. En ocasiones, será vital que contemos con réplicas de algunos recursos para que, dado el caso de un desastre en algún punto de la red, podamos consultar o accesar un recurso similar o de respaldo.

Las compañías también se han dado cuenta que resulta más barato tener una red de computadoras en donde reparten sus procesos productivos que tener una sola supercomputadora en donde concentren todo. Las ventajas de la red son: economía, capacidad de crecimiento más granular, capacidad de soportar fallas, capacidad de tener réplicas más económicas y otras.

1.2. Modelo de referencia OSI

1.2.1 Introducción al Modelo de referencia OSI

El modelo OSI (Open Systems Interconection) de telecomunicaciones esta basado en una propuesta desarrollada por la organización de estándares internacional (ISO), por lo que también se le conoce como modelo ISO (International Standard Organization)-OSI. El modelo OSI establece los lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos. Aunque los fabricantes de hardware y los de software para red son los usuarios principales del modelo OSI, una comprensión general de modelo llega a resultar muy benéfica para el momento en que se expande la red o se conectan redes para formar redes de área amplia (WAN).
Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO dividió el modelo de referencia OSI en capas, entendiéndose por **capa** una entidad que realiza de por sí una función específica.

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 una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

Los criterios que llevaron a este modelo de referencia fueron:

- Deberá crearse una nueva capa siempre que se precise un nuevo grado de abstracción.
- A cada capa deberá asignarse un número bien definido de funciones propias.
- La funcionalidad de cada capa deberá tener en cuenta la posibilidad de definir protocolos normalizados a nivel internacional.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz entre ambas.
- El número de capas será lo suficientemente grande como para no reunir en un nivel funcionalidades distintas y lo suficientemente pequeño para que el resultado final sea manejable en la práctica.

En el modelo de referencia OSI hay siete capas numeradas (figura 1.1), cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Una analogía del sistema de capas puede ser la forma en que una carta es enviada desde el emisor hasta el destinatario. En este proceso intervienen una serie de entidades o capas (carteros, oficinas postales, medios de transporte, etc), cada una de las cuales realiza una serie de funciones específicas, necesarias para el funcionamiento de las demás y para la entrega efectiva de la carta.

Las sietes capas OSI son:

Figura 1.1 Modelo de referencia OSI

1.2.2 Transmisión de datos

Un envío de datos típico bajo el modelo de referencia OSI comienza con una aplicación P en un nodo cualquiera de la red. P genera los datos D que quiere enviar a su contraparte en otro nodo. Le pasa los datos D a la capa de aplicación.
La capa de aplicación toma los datos y los encapsula añadiendo un encabezado que contiene información de control o que puede estar vacío. El paquete completo resultante se lo pasa a la capa de presentación.

La capa de presentación lo recibe y no intenta siquiera decodificar o separar los componentes del paquete, sino que lo toma como datos y le añade un encabezado con información de control de esta capa y el paquete resultante se lo envía a la capa de sesión. La capa de sesión recibe el paquete, que también son sólo datos para ella y le añade un encabezado de control. El resultado se lo envía a la capa de transporte.

La capa de transporte recibe todo el paquete como datos y le añade su propio encabezado de control creando otro paquete que envía a la capa de red, la cual se encargará de enrutarlo a su destino apropiado, entre otras actividades que realiza. Las capas de red, ligado de datos y física toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultada a la capa inferior. La capa física traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.

En el nodo destino, la capa física toma los paquetes y les quita el encabezado de la capa física, pasando el paquete resultante a la capa de ligado de datos. La capa de ligado lo recibe y le quita el encabezado de esta capa, pasando el resultado a la capa de red, quien lo toma y le quita el encabezado de red, pasando el paquete a la capa de transporte que elimina el encabezado de transporte y pasa el resultado a la capa de sesión, quien también le quita el encabezado respectivo y pasa el paquete a la capa de presentación, que a su vez le quita el encabezado de presentación y le pasa el paquete a la capa de aplicación que, finalmente, le quita el último encabezado y le entrega el paquete de datos reales a la aplicación en el nodo destino.

De manera virtual, se establecen conexiones directas entre las capas del mismo nombre de los dos diferentes nodos. Por ejemplo, el paquete que envía la capa de red es interpretado por la capa de red en el destino y no por otra capa. Para las capas inferiores de la de red, dicho paquete fue interpretado como datos, y

para las capas superiores (transporte, sesión, presentación y aplicación) como un paquete compuesto de datos y encabezado.

Por otro lado, todas las capas, excepto la de aplicación, procesan los paquetes realizando operaciones que sólo sirven para verificar que el paquete de datos real esté íntegro o para que éste llegue a su destino, sin que los datos por sí mismos sufran algún cambio.

1.2.2.1. Encapsulamiento

Si un computador A desea enviar datos a otro B, en primer término los datos a enviar se deben colocar en paquetes que se puedan administrar y rastrear, a través de un proceso denominado **encapsulamiento** (Figura 1.2).
Cuando las aplicaciones de usuario envían los datos desde el origen, estos viajan a través de las diferentes capas. Las tres capas superiores (aplicación, presentación y sesión) preparan los datos para su transmisión, creando un formato común para la transmisión. Una vez pasados a este formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tráfico de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

El encapsulamiento consta de los cinco pasos siguientes:

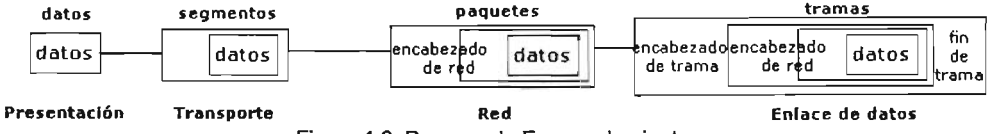


Figura 1.2 Proceso de Encapsulamiento

1. alfanuméricos se convierten en datos que pueden recorrer la red.
2. **Empaquetar los datos** para ser transportados de extremo a extremo (capa transporte). Se dividen los datos en unidades de un tamaño que se pueda administrar (los segmentos), y se les asignan números de secuencia para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. **Agregar la dirección de red al encabezado** (capa de red). El siguiente proceso se produce en la capa de red, que encapsula el segmento creando un paquete o datagrama, agregándole las direcciones lógicas de red de la máquina origen y de la máquina destino. Estas direcciones ayudan a los enrutadores a enviar los paquetes a través de la red por una ruta seleccionada.
4. **Agregar la dirección local al encabezado** de enlace de datos (capa enlace de datos). En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama las direcciones MAC (número de la tarjeta de red, único para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.
5. **Transmitir el tren de bits creado** (Capa física). Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, ondas, etc.). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio, que puede variar a lo largo de la ruta utilizada.

Cuando los datos se transmiten en una red de área local (red LAN), se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es

todo lo que se necesita para llegar desde el host origen hasta el host destino. Pero si se deben enviar los datos a un host de otra red interna o a través de Internet es necesario el uso de paquetes de datos que contengan las direcciones lógicas de las máquinas que se deben comunicar.
Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet.

1.2.2.2. Comunicación entre capas

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como **comunicaciones de par-a-par.** Las reglas y convenciones que controlan esta conversación se denominan **protocolo de la capa n,** y se ocupan del formato y significado de las unidades de datos intercambiadas. Durante este proceso, cada protocolo de capa intercambia unidades de información entre capas iguales de las máquinas que se están comunicando, conocidas con el nombre de **unidades de datos de protocolo** (PDU). Cada capa de comunicación, en el computador origen, se

comunica con un PDU específico de capa y con su capa igual en el computador destino.
También cada capa de un modelo o arquitectura de red recibe **servicios** a la capa que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario. Hay dos tipos principales de servicios:

1. **Servicios orientados a la conexión**: En ellos la conexión es como un tubo a través del cual se envía la información de forma continuada, por lo que los mensajes llegan en el orden que fueron enviados y sin errores. Proporcionan un servicio confiable de comunicación de datos. Una analogía es el sistema telefónico.
2. **Servicios sin conexión**: En los que cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continuada y el ruteo de cada mensaje es independiente. El servicio no es entonces confiable, pues la capa de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

Otra clasificación posible de los servicios en la que distingue entre confiables y no confiables:

- **Servicios confiables**: son aquellos en los que la transmisión de datos está controlada en cada momento, pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos. Para ello la máquina receptora envía mensajes de acuse de recibo de las tramas recibidas a la máquina emisora.
- **Servicios no confiables**: en estos no existe un control de los datos transmitidos, por lo que no se puede garantizar que se hayan recibido todos los datos. Una forma de contrarrestar esta debilidad es la implementación de un sistema de acuse de recibo de las unidades de datos.

En realidad, una capa de una máquina no puede transferir los datos de forma directa a su capa par de otra, si no que necesita los servicios de todas las capas que se encuentran por debajo de ella en la jerarquía de capas, pasándose la información hacia abajo hasta llegar al nivel físico, que es el que realiza el proceso de transferencia de datos.
Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa

necesite para ejecutar su función. De esta forma, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales.
La capa de red presta un servicio a la capa de transporte, trasladando esos datos a través de la red. Para ello encapsula los datos y les agrega un encabezado específico (direcciones lógicas origen y destino), con lo que crea un paquete (PDU de la Capa 3).
La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red (paquetes) en una trama (la PDU de la Capa 2), cuyo encabezado contiene la información necesaria (direcciones físicas) para completar las funciones de enlace de datos.
La capa física también suministra un servicio a la capa de enlace de datos, codificando los datos de la trama de enlace de datos en un patrón de unos y ceros (trenes de bits) para su transmisión a través del medio (generalmente un cable).

1.2.3. Medios de Transmisión

Una vez creadas las señales que nos van a permitir la transmisión de la información, es necesario un puente, un medio físico por el que dichas señales se desplacen desde el host emisor al host destino. Este medio físico puede ser de diferente naturaleza, y la red resultante se clasificará de acuerdo con él, (en capítulos posteriores hablaremos más de los dispositivos de interconexión en una red).

Los tipos principales de medios físicos son el cableado de cobre, el cableado de fibra óptica y la propia atmósfera, usada en transmisiones sin cable, mediante radiofrecuencias, satélites, etc. Generalmente, en redes LAN, que son las que nos ocupan ahora, se usa cableado de cobre, en sus diferentes modalidades, para la unión de host generales, reservándose el uso de cableado de fibra óptica para la unión de nodos principales (backbone).

Cableado de cobre.

El cableado de cobre es, como hemos dicho, el medio más común de unión entre host y dispositivos en redes locales. Los principales tipos de cables de cobre usados son:

1. Cable Coaxial: compuesto por un conductor cilíndrico externo hueco que rodea un solo alambre interno compuesto de dos elementos conductores. Uno de estos elementos (ubicado en el centro del cable) es un conductor de cobre. Está rodeado por una capa de aislamiento flexible. Sobre este material aislador hay una malla de cobre tejida o una hoja metálica que actúa como segundo

alambre del circuito, y como blindaje del conductor interno. Esta segunda capa de blindaje ayuda a reducir la cantidad de interferencia externa, y se encuentra recubierto por la envoltura plástica externa del cable.

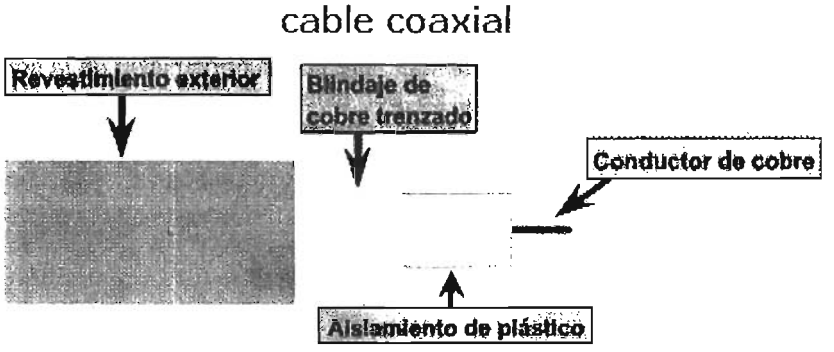


Figura 1.3

Para las LAN, el cable coaxial (Figura 1.3) ofrece varias ventajas. Se pueden realizar tendidos entre nodos de red a mayores distancias que con los cables STP o UTP (unos 500 metros), sin que sea necesario utilizar tantos repetidores. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos.

El cable coaxial viene en distintos tamaños. El cable de mayor diámetro se especificó para su uso como cable de backbone de Ethernet porque históricamente siempre poseyó mejores características de longitud de transmisión y limitación del ruido. Este tipo de cable coaxial frecuentemente se denomina thicknet o red gruesa. Como su apodo lo indica, debido a su diámetro este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. La regla práctica es: cuanto más difícil es instalar los medios de red, más cara resulta la instalación. El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet no se usa casi nunca, salvo en instalaciones especiales.

En el pasado, el cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet o red fina) se usaba para las redes Ethernet. Era particularmente útil para instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet o red barata. Sin embargo, como el cobre exterior o

trenzado metálico del cable coaxial comprende la mitad del circuito eléctrico, se debe tener especial cuidado para garantizar su correcta conexión a tierra. Esto se hace asegurándose de que haya una sólida conexión eléctrica en ambos extremos del cable. Sin embargo, a menudo, los instaladores omiten hacer esto. Como resultado, la mala conexión del blindaje resulta ser una de las fuentes principales de problemas de conexión en la instalación del cable coaxial. Estos problemas producen ruido eléctrico que interfiere con la transmisión de la señal a través de los medios de networking. Es por este motivo que, a pesar de su diámetro pequeño, thinnet ya no se utiliza con tanta frecuencia en las redes Ethernet.

conectores BNC

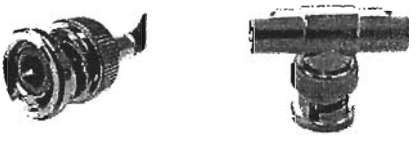


Figura 1.4

Para conectar cables coaxiales se utilizan los conectores BNC (Figura 1.4), simples y en T, y al final del cable principal de red hay que situar unas resistencias especiales, conocidas como resistores, para evitar la reflexión de las ondas de señal.

2. **Par trenzado blindado (STP)**: formado por una capa exterior plástica aislante y una capa interior de papel metálico, dentro de la cual se sitúan normalmente cuatro pares de cables, trenzados para a par, con revestimientos plásticos de diferentes colores para su identificación. Combina las técnicas de blindaje, cancelación y trenzado de cables. Según las especificaciones de uso de las instalaciones de red Ethernet, STP proporciona resistencia contra la interferencia electromagnética y de la radiofrecuencia sin aumentar significativamente el peso o tamaño del cable.

par trenzado blindado STP

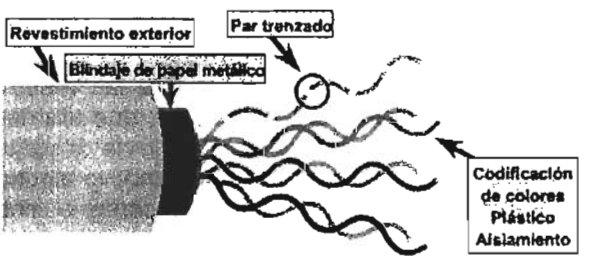


Figura 1.5 Par trenzado blindado STP

El cable de par trenzado (Figura 1.5) blindado tiene las mismas ventajas y desventajas que el cable de par trenzado no blindado. STP brinda mayor protección contra todos los tipos de interferencia externa, pero es más caro que el cable de par trenzado no blindado.

A diferencia del cable coaxial, el blindaje en el STP no forma parte del circuito de datos y, por lo tanto, el cable debe estar conectado a tierra en ambos extremos. Normalmente, los instaladores conectan STP a tierra en el armario para el cableado y el hub, aunque esto no siempre es fácil de hacer, especialmente si los instaladores intentan usar paneles de conexión antiguos que no fueron diseñados para cable STP. Si la conexión a tierra no está bien realizada, el STP puede transformarse en una fuente de problemas, ya que permite que el blindaje actúe como si fuera una antena, absorbiendo las señales eléctricas de los demás hilos del cable y de las fuentes de ruido eléctrico que provienen del exterior del cable.

No es posible realizar tendidos de cable STP tan largos como con otros medios de networking (como, por ejemplo, cable coaxial) sin repetir la señal, siendo la longitud máxima de cable recomendada de unos 100 metros, y su rendimiento suele ser de 10-100 Mbps.

Se especifica otro tipo de STP para instalaciones Token Ring. En este tipo de cable, conocido como STP de 150 ohmios, el cable no sólo está totalmente blindado para reducir la interferencia electromagnética y de radiofrecuencia, sino que a su vez cada par de hilos trenzados se encuentra blindado con respecto a los demás para reducir la diafonía. Si bien el blindaje empleado en el cable de par trenzado blindado de 150 ohmios no forma parte del circuito, como sucede con el cable coaxial, aún así debe estar conectado a tierra en ambos extremos. Este tipo de cable STP requiere una cantidad mayor de aislamiento y de blindaje. Estos factores se combinan para aumentar de manera considerable el tamaño, peso y costo del cable.
También requiere la instalación de grandes armarios y conductos para el cableado, lujos que en muchos edificios antiguos no pueden permitirse.

Para la conexión de los cables STP a los diferentes dispositivos de red se usan unos conectores específicos, denominados conectores STP, similares a los RJ-45 descritos más abajo.

3. **Par trenzado no blindado (UTP)**: compuesto por cuatro pares de hilos, trenzados para a par, y revestidos de un aislante plástico de colores para la identificación de los pares. Cada par de hilos se encuentra aislado de los demás.

Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP (Figura 1.6), la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuanto trenzado se permite por unidad de longitud del cable.

Figura 1.6 Par trenzado no blindado UTP

Cuando se usa como medio de networking, el cable UTP tiene cuatro pares de hilos de cobre de calibre 22 ó 24. El UTP que se usa como medio de networking tiene una impedancia de 100 ohmios. Esto lo diferencia de los otros tipos de cables de par trenzado, como, por ejemplo, los que se utilizan para los teléfonos. Como el UTP tiene un diámetro externo de aproximadamente 0,43 cm, el hecho de que su tamaño sea pequeño puede ser ventajoso durante la instalación. Como el UTP se puede usar con la mayoría de las arquitecturas de networking principales, su popularidad va en aumento.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios de networking. De hecho, el cable UTP cuesta menos por metro que cualquier otro tipo de cableado de LAN, sin embargo, la ventaja real es su tamaño. Como su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Este puede ser

un factor sumamente importante para tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se está instalando el cable UTP con un conector RJ, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad.

Sin embargo, el cableado de par trenzado también tiene una serie de desventajas. El cable UTP es más sensible al ruido eléctrico y la interferencia que otros tipos de medios de networking. Además, en una época el cable UTP

era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable UTP es el más rápido entre los medios basados en cobre.

La distancia máxima recomendada entre repetidores es de 100 metros, y su rendimiento es de 10-100 Mbps.

Para conectar el cable UTP a los distintos dispositivos de red se usan unos conectores especiales, denominados RJ-45 (Registered Jack-45 (Figura 1.7)), muy parecidos a los típicos conectores del cableado telefónico casero.

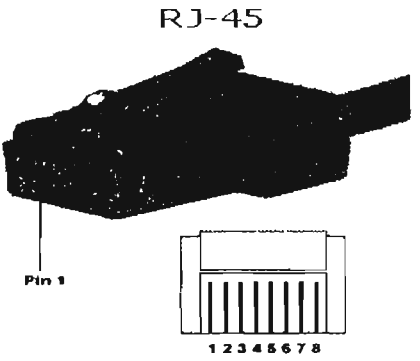


Figura 1.7 RJ-45

Este conector reduce el ruido, la reflexión y los problemas de estabilidad mecánica y se asemeja al enchufe telefónico, con la diferencia de que tiene ocho conductores en lugar de cuatro. Se considera como un componente de networking pasivo ya que sólo sirve como un camino conductor entre los cuatro pares del cable trenzado de Categoría 5 y las patas de la toma RJ-45. Se considera como un componente de la Capa 1, más que un dispositivo, dado que sirve sólo como camino conductor para bits.

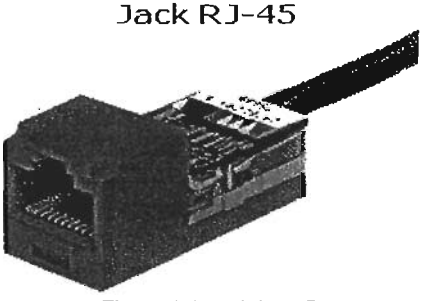


Figura 1.8 Jack RJ-45

Los enchufes o conectores RJ-45 se insertan en jacks o receptáculos RJ-45. Los jacks RJ-45 (Figura 1.8) tienen 8 conductores, que se ajustan a los del conector RJ-45. En el otro lado del jack RJ-45 hay un bloque de inserción donde los hilos individuales se separan y se introducen en ranuras mediante una herramienta similar a un tenedor denominada herramienta de punción.

panel de conexión

Figura 1.9 Panel de control

Para centralizar los diferentes conectores RJ-45 se utilizan unos dispositivos especiales, denominados **paneles de conexión** (Figura 1.9). Vienen provistos de 12, 24 ó 48 puertos y normalmente están montados en un bastidor. Las partes delanteras son jacks RJ-45;, las partes traseras son bloques de punción que proporcionan conectividad o caminos conductores.

4. **Cable de Fibra Óptica**: puede conducir transmisiones de luz moduladas. Si se compara con otros medios de networking, es más caro, sin embargo, no es susceptible a la interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera de los demás tipos de medios de networking descritos aquí. El cable de fibra óptica (Figura 1.10) no transporta impulsos eléctricos, como lo hacen otros tipos de medios de networking que usan cables de cobre. En cambio, las señales que representan a los bits se convierten en haces de luz.

Está compuesto por dos fibras envueltas en revestimientos separados. Si se observa una sección transversal de este cable, veremos que cada fibra óptica se encuentra rodeada por capas de material amortiguador protector, normalmente un material plástico como Kevlar, y un revestimiento externo. El revestimiento exterior protege a todo el cable. Generalmente es de plástico y cumple con los códigos aplicables de incendio y construcción.

cable de fibra óptica

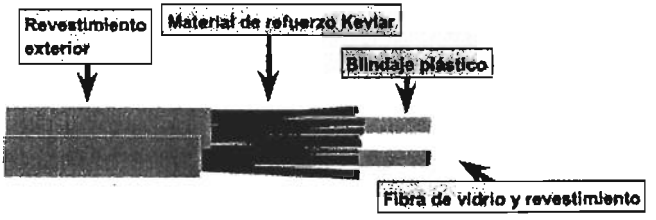


Figura 1.10 Cable de fibra óptica

El propósito del Kevlar es brindar una mayor amortiguación y protección para las frágiles fibras de vidrio que tienen el diámetro de un cabello. Siempre que los códigos requieran que los cables de fibra óptica deban estar bajo tierra, a veces se incluye un alambre de acero inoxidable como refuerzo.

Las partes que guían la luz en una fibra óptica se denominan núcleo y revestimiento. El núcleo es generalmente un vidrio de alta pureza con un alto índice de refracción Cuando el vidrio del núcleo está recubierto por una capa de revestimiento de vidrio o de plástico con un índice de refracción bajo, la luz se captura en el núcleo de la fibra. Este proceso se denomina reflexión interna total y permite que la fibra óptica actúe como un "tubo de luz", guiando la luz a través de enormes distancias, incluso dando vuelta en codos. La longitud máxima de cable recomendada entre nodos en de 2.000 metros, y su rendimiento es alto, de 100 0 más Mbps.

5. **Medios inalámbricos**: se basan en la transmisión de ondas electromagnéticas, que pueden recorrer el vacío del espacio exterior y medios como el aire, por lo que no es necesario un medio físico para las señales inalámbricas, lo que hace que sean un medio muy versátil para el desarrollo de redes. Veamos los siguientes medios de transmisión inalámbricos.

Microondas terrestres.

La antena utilizada generalmente en las microondas es la de tipo parabólico. El tamaño típico es de un diámetro de unos 3 metros. La antena es fijada rígidamente, y transmite un haz estrecho que debe estar perfectamente enfocado hacia la antena receptora. Estas antenas de microondas se deben ubicar a una altura considerable sobre el nivel del suelo, con el fin de conseguir mayores separaciones posibles entre ellas y poder superar posibles obstáculos. Sin obstáculos intermedios la distancia máxima entre antenas es de aproximadamente 7.14 Km, claro esta que esta distancia se puede extender, si se aprovecha la característica de curvatura de la tierra, por medio de la cual las microondas se desvían o refractan en la atmósfera terrestre.

Las transmisiones a larga distancia se llevan a cabo, mediante la concatenación de enlaces punto a punto entre torres adyacentes, hasta cubrir la distancia deseada. El uso principal de los sistemas de microondas terrestres son los servicios de telecomunicación de larga distancia, como alternativa al cable coaxial o a las fibras ópticas. La utilización de microondas requiere menor número de repetidores o amplificadores que el cable coaxial, pero en cambio necesita que las antenas estén alineadas. El uso de microondas es frecuente en la transmisión de televisión y voz. Otro de los usos que se le pueden dar a las

microondas, es el de enlaces punto a punto entre edificios. En los enlaces entre edificios, se pueden emplear para circuitos cerrados de televisión o para interconexión de redes locales.

El rango de las microondas cubre una parte sustancial del espectro. La banda de frecuencias esta comprendida entre 2 y 40 GHz.

Cuanto mayor sea la frecuencia utilizada, mayor el ancho de banda potencial, y por consiguiente mayor es virtualmente la velocidad de transmisión. En el cuadro 2, se indican los valores frecuentes de anchos de banda y velocidad de transmisión de datos para algunos sistemas típicos.

Microondas por satélite.

A diferencia de las microondas terrestres, las microondas satelitales lo que hacen básicamente, es retransmitir información, se usa como enlace entre dos o más transmisores/receptores terrestres, denominados estaciones base. El satélite funciona como un espejo sobre el cual la señal rebota, su principal función es la de amplificar la señal, corregirla y retransmitirla a una o más antenas ubicadas en la tierra. Los satélites geoestacionarios (es decir permanecen inmóviles para un observador ubicado en la tierra), operan en una serie de frecuencias llamadas transponders, es importante que los satélites se mantengan en una órbita geoestacionaria, porque de lo contrario estos perderían su alineación con respecto a las antenas ubicadas en la tierra.

Como se mencionó anteriormente la transmisión satelital, puede ser usada para proporcionar una comunicación punto a punto entre dos antenas terrestres alejadas entre si, o para conectar una estación base transmisora con un conjunto de receptores terrestres. Si dos satélites utilizan la misma banda de frecuencias y se encuentran lo suficientemente próximos, estos podrían interferirse mutuamente, por lo que es necesario que estén separados por lo menos 4 grados (desplazamiento angular medio desde la superficie terrestre), en la banda 4/6 GHz, y una separación de al menos 3 grados a 12/14 GHz, por tanto el número máximo de satélites posibles esta bastante limitado.

Las comunicaciones satelitales son una revolución tecnológica de igual magnitud que las fibras ópticas, entre las aplicaciones más importantes para los satélites tenemos: Difusión de televisión, transmisión telefónica a larga distancia y redes privadas entre otras. Debido a que los satélites por lo general son multidestino, su utilización es muy adecuada para distribución de televisión, por lo que están siendo ampliamente utilizadas en Estados Unidos y el resto del mundo.

La comunicación vía satélite se utiliza también para proporcionar enlaces punto a punto entre las centrales telefónicas en las redes publicas de telefonía.

Finalmente, para la tecnología vía satélite hay una gran cantidad de aplicaciones de gran interés comercial, el suministrador del servicio de transmisión vía satélite puede dividir la capacidad total disponible en una serie de canales, alquilando su uso a terceras compañías.

El rango de frecuencias óptimo para la transmisión vía satélite esta en el intervalo comprendido entre 1 y 10 GHz. Por debajo de 1 GHz, el ruido producido por causas naturales es apreciable, incluyendo el ruido galáctico, solar, atmosférico y el producido por interferencias con otros dispositivos electrónicos.

Espectro infrarrojo (IR)

Es la zona de infrarrojos del espectro que va en términos generales desde los 3 x 1011 hasta los 2 x 1014Hz. Los infrarrojos son útiles para las conexiones locales punto a punto así como para aplicaciones multipunto dentro de áreas de cobertura limitada como por ejemplo una habitación.

Una diferencia significativa entre la transmisión de rayos infrarrojos y las microondas es que los primeros no pueden atravesar paredes. Por tanto los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este tipo de transmisión. Es más, no hay problemas de asignación de frecuencias, ya que en esta banda no se necesitan permisos. Por su naturaleza y características de transmisión la tecnología infrarroja es utilizada en aplicaciones LAN verticales (como las médicas o de inventario de almacenes), clientes conectándose en grandes áreas abiertas, impresión inalámbrica y la transferencia de archivos. La velocidad de transmisión máxima alcanzada hasta ahora es de 10 Mbps. La cobertura de este tipo de tecnología esta limitada a LAN o campus si se utilizan repetidores inalámbricos y puentes. Entre las ventajas que podemos resaltar es una mayor velocidad que las de amplio espectro, y su inmunidad a la interferencia de fuentes de radiofrecuencia. Pero por el contrario de las otras tecnologías, como se mencionó anteriormente la tecnología de espectro infrarrojo, no puede penetrar paredes y además su rango de alcance es bastante corto.

La IrDA (Infrared Data Association), es un grupo de manufacturadores de dispositivos que desarrollaron un estándar para la transmisión de datos vía ondas de luz infrarrojas. Recientemente, los computadores y otros dispositivos (como impresoras), vienen con puertos IrDA. Estos puertos habilitan los dispositivos para transferir información de forma inalámbrica. Por ejemplo si

ambos dispositivos (computador e impresora), están equipados con esta tecnología, simplemente se alinean ambos, y ya esta, usted ahora tiene comunicación entre su computador y la impresora.

Transmisión por ondas de luz

La señalización óptica por medio de guías se ha usado durante siglos. Paul Rivere utilizó señalización óptica binaria desde la vieja Iglesia del Norte justo antes de su famoso viaje. Una aplicación más moderna es conectar las LAN de dos edificios por medio de láseres montados en sus azoteas. La señalización óptica coherente con láseres es inherentemente unidireccional, de modo que cada edificio necesita su propio láser y su propio fotodetector, este esquema proporciona un ancho de banda muy alto y un costo muy bajo. También es relativamente fácil de instalar y, a diferencia de las microondas, no requiere un licencia de la FCC (Comisión Federal de Comunicaciones).

La ventaja del láser, un haz muy estrecho, es aquí también una debilidad. Apuntar un rayo láser de 1 mm a 500 metros de distancia, requiere de una gran precisión, por lo general se le añaden lentes al sistema para desenfocar ligeramente el rayo. Una desventaja de los rayos láser es que no pueden atravesar la niebla, ni la lluvia normalmente funcionan bien en los días soleados.

Ondas de radio

Las ondas de radio son fáciles de generar, pueden viajar distancias muy largas y penetrar edificios sin problema, de modo que se utilizan mucho en la comunicación tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viajan en todas las direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse físicamente.

Básicamente hay dos tipos de transmisiones inalámbricas:

Direccional.

También llamada sistemas de banda angosta (narrow band (Figura 1.11)) o de frecuencia dedicada, la antena de transmisión emite la energía electromagnética en un haz; por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas.

Para que la transmisión pueda ser enviada en una dirección especifica, debemos tener en cuenta la frecuencia, la cual debe ser mucho mayor que la utilizada en transmisiones omnidireccionales.

Figura 1.11 Transmisión inalámbrica Direccional

Omnidireccional

O también llamados sistemas basados en espectro disperso o extendido (spread spectrum) (Figura 1.12), al contrario que las direccionales, el diagrama de radiación de la antena es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general cuanto mayor es la frecuencia de la señal transmitida es más factible concentrar la energía en un haz direccional.

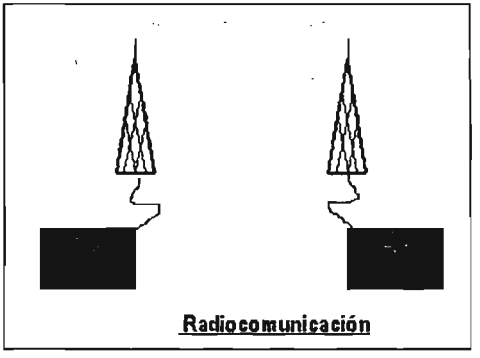


Figura 1.12 Transmisión inalámbrica Omnidireccional

1.2.4 Descripción de las capas del Modelo OSI.

Capa 7: La capa de aplicación.
La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos las aplicaciones de usuario acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.
Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa 6: La capa de presentación.

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.
Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.

Es también las responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.
Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traduce entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.
- Define la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.

- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Da formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario.
- Aplica a los datos procesos criptográficos cuando sea necesario.

Capa 5: La capa de sesión.

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos hosts (máquinas en red) que se están comunicando.

Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin perdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, chequeando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.

- Sincronizar el diálogo entre las capas de presentación de los dos hosts y administrar su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre máquinas, regulando quien habla y por cuanto tiempo.
- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar **tokens** . Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación, base de ciertos tipos de redes, como Token Ring o FDDI.
- Hacer **checkpoints**, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

Capa 4: La capa de transporte.

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión.
Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas **segmentos**, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.
La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte confiable de datos entre los nodos de la red.
Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Se conocen con el nombre de **circuitos virtuales** a las conexiones que se establecen dentro de una red. En ellos no hay la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.
Podemos resumir las funciones de la capa de transporte en los siguientes puntos:

- Controlar la interacción entre procesos usuarios en las máquinas que se comunican.
- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y el direccionamiento de procesos de maquina a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte confiable, llamadas segmentos, que pasa luego a la capa de red para su envío.
- Realizar funciones de control y numeración de las unidades de información (los segmentos).
- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.
- Garantizar la transferencia de información a través de la red.

Capa 3: La capa de red.

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la

comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

Sus principales funciones son:

- Dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas **paquetes**, a los que asigna las direcciones lógicas de los host que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Encaminar la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Ensamblar los paquetes en el host destino.

En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

Capa 2: La capa de enlace de datos.

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo, realizando para ello las siguientes funciones:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.
- Agregar una secuencia especial de bits al principio y al final de los paquetes de datos, estructurando este flujo bajo un formato predefinido, denominado **trama**, que suele ser de unos cientos de bytes.

- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan **CRC** (Códigos Cíclicos Redundantes) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.
- Controlar la congestión de la red.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Encargarse del acceso de los datos al medio (soportes físicos de la red).

Capa 1: La capa física.

La Capa Física es la capa que define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, ocupándose de las transmisiones a nivel de bit.

Las funciones principales de la Capa Física son:

- Permitir la compatibilidad entre los diferentes tipos de conectores existentes.
- Definir las funciones que van a realizar cada uno de los pines de los conectores.
- Establecer el tipo de cableado que se debe usar en la red.
- Determinar la codificación, el voltaje de las señales y la duración de los pulsos eléctricos.
- Coordinar la modulación de las señales, si es necesario.
- Amplificar y retemporizar las señales en su viaje a través de los medios.

Por lo tanto, incluye todos y cada uno de los elementos de red encargados de transformar los trenes de bits de las tramas en señales aptas de ser transportadas por los medios físicos y viceversa, los medios físicos en sí (cableado de cualquier tipo), los diferentes conectores de unión entre cables y dispositivos de red y los propios dispositivos que trabajan a nivel de impulsos y señales eléctricas (repetidores, hubs, etc.).

El párrafo anterior resume las operaciones generales que van a producirse en la Capa Física, y que detallo a continuación:

1. Las tramas formadas en la Capa de Enlace de Datos se unen una tras otra en lo que se conoce como "trenes de bits", sucesiones de ceros y unos lógicos que contienen toda la información necesaria para la comunicación de datos entre dos

host. Estos trenes de bits deben ser convertidos en señales estándares capaces de viajar de forma correcta por los sucesivos **cables** (y atmósfera, en el caso de redes inalámbricas) que van a unir los host emisor y receptor, es decir, en impulsos eléctricos adecuados para la transmisión de datos.
Generalmente, esta conversión bits-señales se lleva a cabo en ciertos chips constituyentes de la **tarjeta de red** del host emisor o en dispositivos especiales para tal fin, como los **módems**. Es por esto que en realidad debemos considerar las tarjetas de red como dispositivos pertenecientes tanto a la Capa de Enlace de Datos como a la Capa Física.

2. Una vez creadas las señales, estas deben ser encaminadas a través del cableado que une los host emisor y destinatario. Para ello se precisan unos elementos de unión entre las placas madre de los host, las tarjetas de red o los módems y los cables en sí, elementos que pueden variar de una implementación de red a otra. Ejemplo de estos elementos de unión son los famosos **conectores RJ-45** y los **Jacks RJ-45** del cableado de par trenzado y los **conectores en T** de los cables coaxiales.

3.Las señales viajan por los diferentes cables que forman la red o redes intermedias entre los host que se comunican. Pero puede suceder que las diferentes redes sean de topología diferente, por lo que habrá que disponer de elementos capaces de transformar un tipo de señales en otro. Estos elementos se denominan **transceptores**, y forman también parte de la Capa Física.

4. Si la longitud de cableado que deben recorrer las señales es superior a unos determinados límites (que generalmente son de no muchos metros - 90 o 100 en el caso de cableado de par trenzado,
por ejemplo-) será necesario amplificar y retemporizar las mismas, ya que perderán intensidad y claridad en el recorrido, llegando a hacerse ininteligibles. Para esta tarea se utilizan dispositivos especiales de red que actúan sobre las señales, denominados **repetidores** y **hubs**.

5. Una vez las señales llegan al host destino, el proceso de codificación se invierte, transformando las señales recibidas en trenes de bits, capaces de ser interpretados por la pila de protocolos superiores, de tal forma que se recupere el mensaje original.
Vamos pues a estudiar a continuación todo este proceso de forma más detallada (salvo los dispositivos de red, a los que dedicaremos un capítulo aparte), procurando no entrar en demasiadas consideraciones científicas, aunque será necesaria la explicación de algún factor técnico necesario.

1.3. Conceptos Básicos

1.3.1. Red de computadoras

Una red está formada por una serie de estaciones de trabajo, coordinadas por unas máquinas especiales, denominadas servidores, y por una conjunto variable de dispositivos autónomos, como impresoras, escáneres, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs. Cada dispositivo activo que interviene en la comunicación de forma autónoma se denomina nodo.
Todos ellos se comunican entre sí directamente por medios de transmisión físicos (cables coaxiales, de par trenzado o de fibra óptica) o basados en ondas (redes inalámbricas), aunque si el tamaño de la red lo exige pueden hacerlo mediante líneas telefónicas, de radio de largo alcance o por satélite.

Los sistema de comunicación en red se basan en la **arquitectura cliente-servidor** (Figura 1.13) , que es una forma específica de diseño de aplicaciones, aunque también se conoce con este nombre a los ordenadores en los que estas aplicaciones se están ejecutando. Así,

el cliente es el ordenador que se encarga de efectuar una petición o solicitar un servicio, mientras que el servidor es el ordenador remoto que controla dichos servicios y que se encarga de evaluar la petición del cliente y de decidir si ésta es aceptada o rechazada, y si es aceptada, de proporcionar dichos datos al cliente.
Hay que tener en cuenta que cliente y servidor no tienen porque estar en ordenadores separados, ya que pueden ser programas diferentes que se están ejecutando en un mismo computador.

Arquitectura cliente-servidor

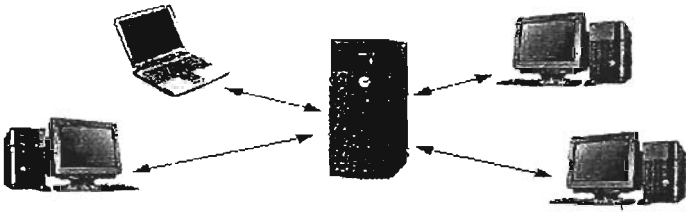


Figura 1.13 Arquitectura cliente-servidor

A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas, etc. Esta comunicación de

datos se realiza mediante el envío de unidades de información, lógicamente agrupadas, denominadas **paquetes de datos** .

Los paquetes de datos incluyen la información origen junto con otros elementos necesarios para hacer que la comunicación sea factible y confiable en relación con los dispositivos destino. La dirección origen de un paquete especifica la identidad del computador que envía el paquete. La dirección destino especifica la identidad del computador que finalmente recibe el paquete.
Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o **protocolo** . Un protocolo es una descripción formal de un conjunto de normas y convenciones que determinan el formato y la transmisión de los datos entre los diferentes dispositivos de una red.

Todo protocolo debe definir los siguientes aspectos en la comunicación de datos:

- Sintaxis: el formato de los datos y los niveles de la señal.
- Semántica: información de control para la coordinación y el manejo de errores.
- Temporización: sincronización de velocidades de secuenciación.

Otro concepto importante es el de **interfaz**, aunque puede resultar complicado de explicar, ya que admite varias definiciones:

- Una interfaz entre equipos es el mecanismo encargado de la conexión física entre ellos, definiendo las normas para las características eléctricas y mecánicas de la conexión.
- Una interfaz entre capas es el mecanismo que hace posible la comunicación entre dichas capas, de forma independiente a las mismas (según esto, entre cada dos capas del modelo OSI habrá una interfaz de comunicación).

Y a todos nos suena el concepto de interfaz de usuario, que en cualquier aplicación es el sistema por el cual ésta se comunica con el usuario e interactúa con él.

1.3.2. Clasificación de redes

Como ya hemos visto, se denomina red de computadores una serie de host autónomos y dispositivos especiales intercomunicados entre sí.
Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de las mismas, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

La posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

Clasificación de las redes según su tamaño y extensión:

1. **Redes LAN**. Las redes de área local (Local Area Network) son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).
2. **Redes MAN**. Las redes de área metropolitana (Metropolitan Area Network) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.
3. **Redes WAN**. Las redes de área amplia (Wide Area Network) tienen un tamaño superior a una MAN, y consisten en una colección de host o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un router a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros.
4. **Redes internet**. Una internet es una red de redes, vinculadas mediante ruteadores gateways. Un gateway o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10000 kilómetros en adelante, y su ejemplo más claro es Internet, la red de redes mundial.
5. **Redes inalámbricas**. Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Clasificación de las redes según la tecnología de transmisión:

a. **Redes de Broadcast**. Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartido entonces por

todas las máquinas de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red.

b. **Redes Point-To-Point**. Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. Para poder transmitir los paquetes desde una máquina a otra a veces es necesario que éstos pasen por máquinas intermedias, siendo obligado en tales casos un trazado de rutas mediante dispositivos routers.

Clasificación de las redes según el tipo de transferencia de datos que soportan:

I. **Redes de transmisión simple**. Son aquellas redes en las que los datos sólo pueden viajar en un sentido.
II. **Redes Half-Duplex**. Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.
III. **Redes Full-Duplex**. Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

1.3.3. Topologías de redes

Hemos visto en el tema sobre el modelo OSI que las redes de ordenadores surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos.
Checar
Pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de **topología de la red**. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

- La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.
- La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

- La topología matemática, mapas de nodos y enlaces, a menudo formando patrones.

La topología de broadcast simplemente significa que cada host envía sus datos hacía todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.
Vamos a ver a continuación los principales modelos de topología.

1.3.3.1. Topología de Bus

La topología de bus (Figura 1.14) tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados. La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información.

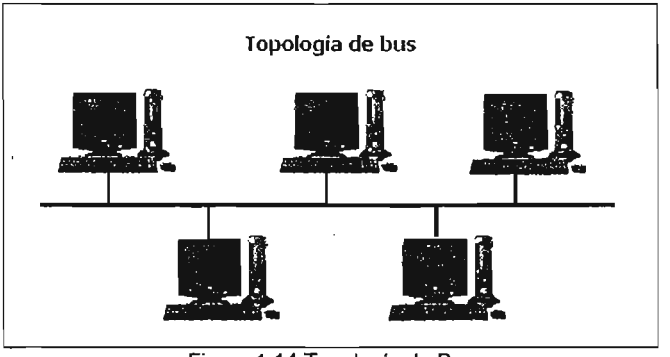


Figura 1.14 Topología de Bus

Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

1.3.3.2. Topología de anillo

Una topología de anillo (Figura 1.15) se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

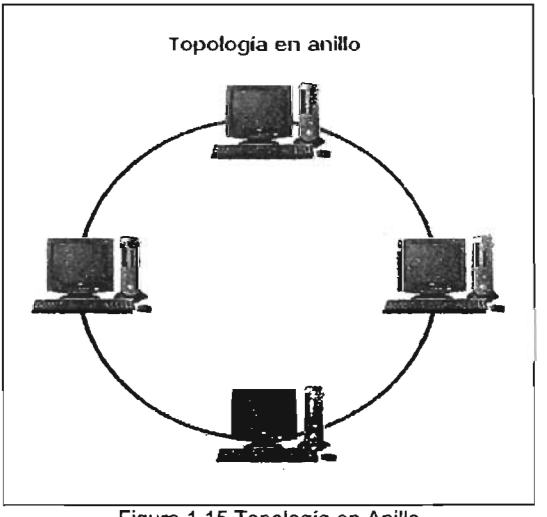


Figura 1.15 Topología en Anillo

1.3.3.3. Topología de anillo doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos.

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

1.3.3.4. Topología en estrella

La topología en estrella (Figura 1.16) tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

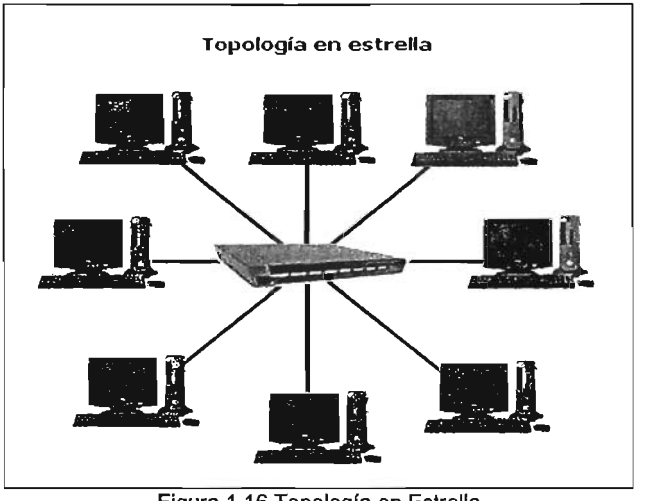


Figura 1.16 Topología en Estrella

1.3.3.5. Topología en estrella extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

1.3.3.6. Topología en árbol

La topología en árbol (Figura 1.17), es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

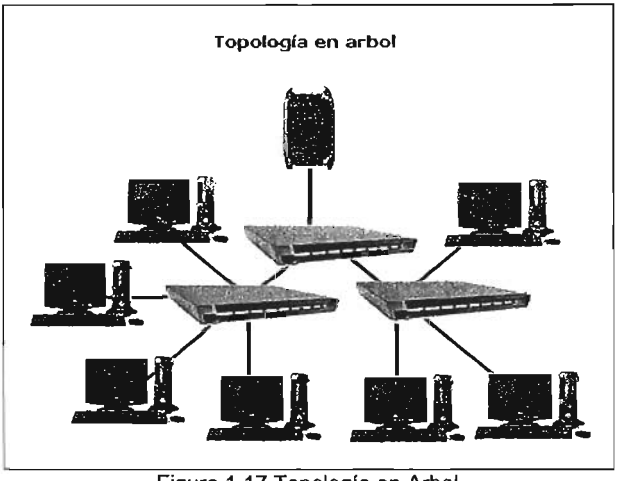


Figura 1.17 Topología en Arbol

1.3.3.7. Topología en malla completa

En una topología de malla completa (Figura 1.18), cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

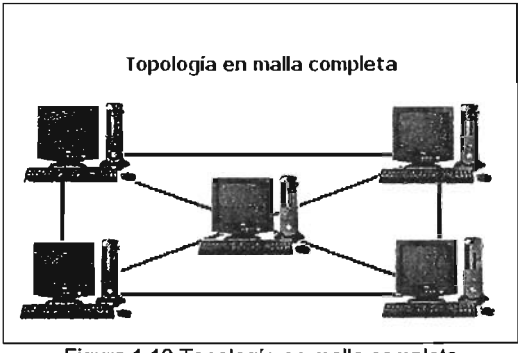


Figura 1.18 Topología en malla completa

1.3.3.8..Topología de red celular

La topología celular (Figura 1.19), está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.
Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

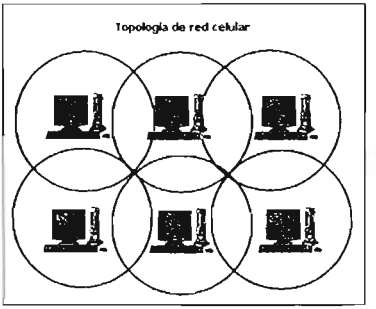


Figura 1.19 Topología de red celular

1.3.3.9. Topología irregular

En este tipo de topología no existe un patrón obvio de enlaces y nodos. El cableado no sigue un modelo determinado; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera.
Las topologías LAN más comunes son:

- **Ethernet**: topología de bus lógica y en estrella física o en estrella extendida.
- **Token Ring**: topología de anillo lógica y una topología física en estrella.
- **FDDI**: topología de anillo lógica y topología física de anillo doble.

Vamos a verlas más detenidamente.

1.3.3.10. Topologías LAN

1.3.3.10.1 Redes LAN Ethernet

Ethernet es la tecnología de red LAN más usada, resultando idóneas para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10-100 Mbps.

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo, en los años setenta, el **Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD** (Carrier Sense

and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor encada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

El centro de investigaciones PARC (Palo Alto Research Center) de la Xerox Corporation desarrolló el primer sistema Ethernet experimental en los años 70, que posteriormente sirvió como base de la especificación 802.3 publicada en 1980 por el Institute of Electrical and Electronic Engineers (IEEE).

Las redes Ethernet son de carácter no determinista, en la que los hosts pueden transmitir datos en cualquier momento. Antes de enviarlos, escuchan el medio de transmisión para determinar si se encuentra en uso. Si lo está, entonces esperan. En caso contrario, los host comienzan a transmitir. En caso de que dos o más host empiecen a transmitir tramas a la vez se producirán encontronazos o choques entre tramas diferentes que quieren pasar por el mismo sitio

a la vez. Este fenómeno se denomina **colisión**, y la porción de los medios de red donde se producen colisiones se denomina **dominio de colisiones**.

Una colisión se produce pues cuando dos máquinas escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde.

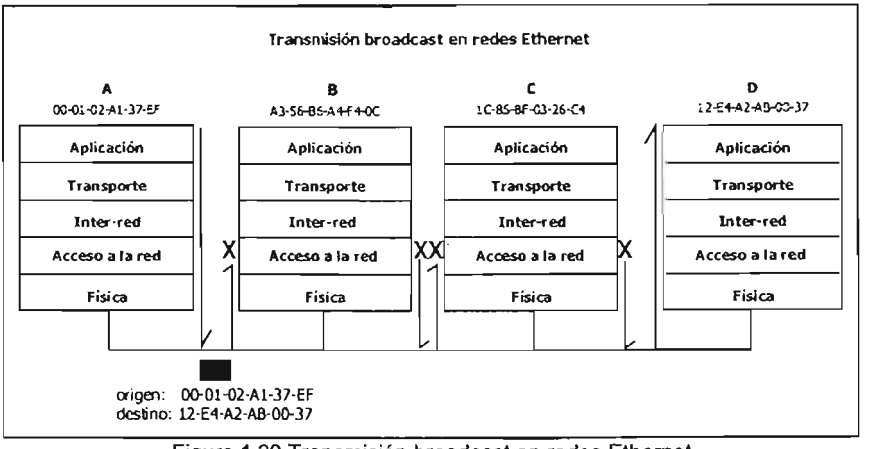


Figura 1.20 Transmisión broadcast en redes Ethernet

Para intentar solventar esta pérdida de paquetes, las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación que determinan el momento en que aquellas que han enviado tramas que han sido destruidas por colisiones pueden volver a transmitirlas.

Existen dos especificaciones diferentes para un mismo tipo de red, Ethernet y IEEE 802.3. Ambas son **redes de broadcast** (Figura 1.20), lo que significa que cada máquina puede ver todas las tramas, aunque no sea el destino final de las mismas. Cada máquina examina cada trama que circula por la red para determinar si está destinada a ella. De ser así, la trama pasa a las capas superiores para su adecuado procesamiento. En caso contrario, la trama es ignorada.

Ethernet proporciona servicios correspondientes a las capas físicas y de enlace de datos del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física y la porción de acceso al canal de la capa de enlace de datos, pero no define ningún protocolo de Control de Enlace Lógico.

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos.
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.>
3. Detectar errores dentro de los paquetes de datos o en la red.

Tanto Ethernet como IEEE 802.3 se implementan a través de la **tarjeta de red** o por medio de circuitos en una placa dentro del host.

Formato de trama Ethernet

Según he explicado, los datos generados en la capa de aplicación pasan a la capa de transporte, que los divide en segmentos, porciones de datos aptas para su transporte por res, y luego van descendiendo pos las sucesivas capas hasta llegar a los medios físicos. Conforme los datos van bajando por la pila de capas, paso a paso cada protocolo les va añadiendo una serie de cabeceras y datos adicionales; necesarios para poder ser enviados a su destino correctamente. El resultado final es una serie de unidades de información denominadas tramas (Figura 1.21), que son las que viajan de un host a otro.

La forma final de la trama obtenida, en redes Ethernet, es la siguiente:

Trama Ethernet

cabecera Ethernet	cabecera IP (20 bytes)	cabecera TCP (20 bytes)	datos	checksum Ethernet

Figura 1.21 Trama Ethernet

Y los principales campos (Figura 1.22), que la forman son:

Campos de la trama Ethernet

7	1	6	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección Destino	Dirección Origen	Tipo	Datos	Secuencia de verificación de trama

Figura 1.22 Campos de la trama Ethernet

- Preámbulo: Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.
- Inicio de trama (SOF): Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.
- Direcciones destino y origen: Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).
- Tipo (Ethernet): Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.
- Longitud (IEEE 802.3): Indica la cantidad de bytes de datos que sigue este campo.
- Datos: Incluye los datos enviados en la trama. En las especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.

- Secuencia de verificación de trama (FCS): Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese. El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes.

Tipos de redes Ethernet

Existen por lo menos 18 variedades de Ethernet (Figura 1.23), relacionadas con el tipo de cableado empleado y con la velocidad de transmisión.

Variedades de red Ethernet

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

Figura 1.23 Variedades de red Ethernet

Las tecnologías Ethernet más comunes y más importantes las son:

- **Ethernet 10Base2.** Usa un cable coaxial delgado, por lo que se puede doblar más fácilmente, y además es más barato y fácil de instalar, aunque los segmentos de cable no pueden exceder de 200 metros y 30 nodos.

Las conexiones se hacen mediante *conectores en T*, más fáciles de instalar y más seguros.

- **Ethernet 10Base5.** También llamada Ethernet gruesa, usa un cable coaxial grueso, consiguiendo una velocidad de 10 Mbps. Puede tener hasta 100 nodos conectados, con una longitud de cable de hasta 500 metros. Las conexiones se hacen mediante la técnica denominada *derivaciones de vampiro*, en las cuales se inserta un polo hasta la mitad del cable, realizándose la derivación en el interior de un transceiver, que contiene los elementos necesarios para la detección de portadores y choques. El transceiver se une al computador mediante un cable de hasta 50 metros.
- **Ethernet 10Base-T.** Cada estación tiene una conexión con un hub central, y los cables usados son normalmente de par trenzado. Son las LAN más comunes hoy en día. Mediante este sistema se palian los conocidos defectos de las redes 10BAse2 y 10Base5, a saber, la mala detección de derivaciones no deseadas, de rupturas y de conectores flojos. Como desventaja, los cables tienen un límite de sólo 100 metros, y los hubs pueden resultar caros.

- **Ethernet 10Base-FX.** Basada en el uso de fibra óptica para conectar las máquinas, lo que la hace cara para un planteamiento general de toda la red, pero idónea para la conexión entre edificios, ya que los segmentos pueden tener una longitud de hasta 2000 metros, al ser la fibra óptica insensible a los ruidos e interferencias típicos de los cables de cobre. Además, su velocidad de transmisión es mucho mayor.

- **Fast Ethernet**. Las redes 100BaseFx (IEEE 802.3u) se crearon con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10Base-T y buscar una alternativa a las redes FDDI Son también conocidas como redes Fast Ethernet, y están basadas en una topología en estrella para fibra óptica. Con objeto de hacerla compatible con Ethernet 10Base-T, la tecnología Fast Ethernet preserva los formatos de los paquetes y las interfaces, pero aumenta la rapidez de transmisión hasta los 100 Mbps. En la redes Fast Ethernet se usan cables de cuatro pares trenzados de la clase 3, uno de los cuales va siempre al hub central, otro viene siempre desde el hub, mientras que los otros dos pares son conmutables. En cuanto a la codificación de las señales, se sustituye la codificación Manchester por señalización temaria, mediante la cual se pueden transmitir 4 bits a la vez. También se puede implementar Fast Ethernet con cableado de la clase 5 en topología de estrella (100BaseTX), pudiendo entonces soportar hasta 100 Mbps con transmisión full dúplex.

1.3.3.10.2. Redes LAN Token Ring

Las redes Token Ring (Figura 1.24), son redes de tipo determinista, al contrario de las redes Ethernet. En ellas, el acceso al medio está controlado, por lo que solamente puede transmitir datos una máquina por vez, implementándose este control por medio de un token de datos, que define qué máquina puede transmitir en cada instante. Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens.

Las redes de transmisión de tokens se implementan con una topología física de estrella y lógica de anillo, y se basan en el transporte de una pequeña trama, denominada token, cuya posesión otorga el derecho a transmitir datos. Si un nodo que recibe un token no tiene información para enviar, transfiere el token al siguiente nodo. Cada estación puede mantener al token durante un período de tiempo máximo determinado, según la tecnología específica que se haya implementado.

Cuando una máquina recibe un token y tiene información para transmitir, toma el token y le modifica un bit, transformándolo en una secuencia de inicio de trama. A continuación, agrega la información a transmitir a esta trama y la envía al anillo, por el que gira hasta que llega a la estación destino.
Mientras la trama de información gira alrededor del anillo no hay ningún otro token en la red, por lo que ninguna otra máquina puede realizar transmisiones.

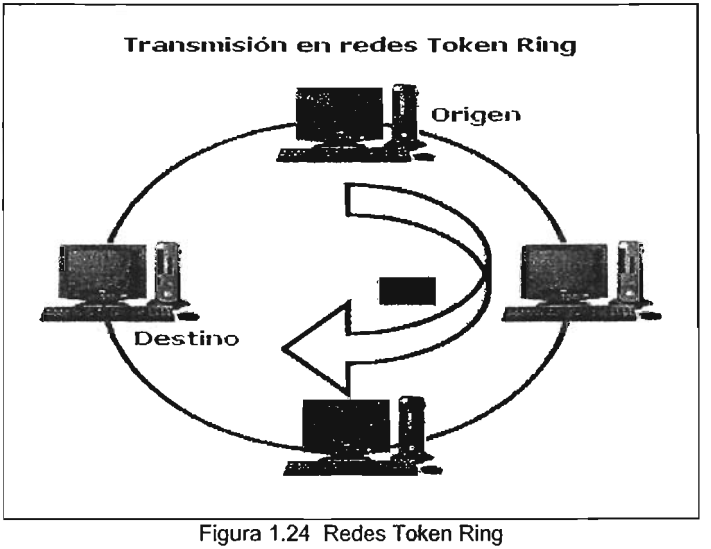


Figura 1.24 Redes Token Ring

Cuando la trama llega a la máquina destino, ésta copia la información contenida en ella para su procesamiento y elimina la trama, con lo que la estación emisora puede verificar si la trama se recibió y se copió en el destino.

Como consecuencia de este método determinista de transmisión, en las redes Token Ring no se producen colisiones, a diferencia de las redes CSMA/CD como Ethernet. Además, en las redes Token Ring se puede calcular el tiempo máximo que transcurrirá antes de que cualquier máquina pueda realizar una transmisión, lo que hace que sean ideales para las aplicaciones en las que cualquier demora deba ser predecible y en las que el funcionamiento sólido de la red sea importante.

La primera red Token Ring fue desarrollada por la empresa IBM en los años setenta, todavía sigue usándose y fue la base para la especificación IEEE 802.5 (método de acceso Token Ring), prácticamente idéntica y absolutamente compatible con ella. Actualmente, el término Token Ring se refiere tanto a la red Token Ring de IBM como a la especificación 802.5 del IEEE.
Las redes Token Ring soportan entre 72 y 260 estaciones a velocidades de 4 a 16 Mbps, se implementan mediante cableado de par trenzado, con blindaje o sin él, y utilizan una señalización de banda base con codificación diferencial de Manchester.

Tokens

Los tokens (Figura 1.25) están formados por un byte delimitador de inicio, un byte de control de acceso y un byte delimitador de fin. Por lo tanto, tienen una longitud de 3 bytes.

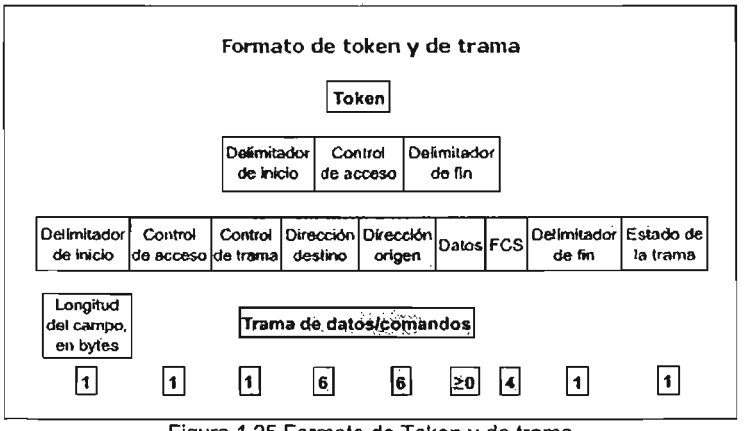


Figura 1.25 Formato de Token y de trama

- El delimitador de inicio alerta a cada estación ante la llegada de un token o de una trama de datos/comandos. Este campo también incluye señales que distinguen al byte del resto de la trama al violar el esquema de codificación que se usa en otras partes de la trama.
- El byte de control de acceso contiene los campos de prioridad y de reserva, así como un bit de token y uno de monitor. El bit de token distingue un token de una trama de datos/comandos y un bit de monitor determina si una trama gira continuamente alrededor del anillo.
- El delimitador de fin señala el fin del token o de una trama de datos/comandos. Contiene bits que indican si hay una trama defectuosa y una trama que es la última de una secuencia lógica.

El tamaño de las tramas de datos/comandos varía según el tamaño del campo de información. Las tramas de datos transportan información para los protocolos de capa superior, mientras que las tramas de comandos contienen información de control y no poseen datos para los protocolos de capa superior.

En las tramas de datos o instrucciones hay un byte de control de trama a continuación del byte de control de acceso. El byte de control de trama indica si la trama contiene datos o información de control. En las tramas de control, este byte especifica el tipo de información de control.

A continuación del byte de control de trama hay dos campos de dirección que identifican las estaciones destino y origen. Como en el caso de IEEE 802.5, la longitud de las direcciones es de 6 bytes. El campo de datos está ubicado a continuación del campo de dirección. La longitud de este campo está limitada por el token de anillo que mantiene el tiempo, definiendo de este modo el tiempo máximo durante el cual una estación puede retener al token.

Y a continuación del campo de datos se ubica el campo de secuencia de verificación de trama (FCS). La estación origen completa este campo con un valor calculado según el contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado mientras estaba en tránsito. Si la trama está dañada se descarta. Como en el caso del token, el delimitador de fin completa la trama de datos/comandos.

Sistema de prioridad

Las redes Token Ring usan un sistema de prioridad sofisticado que permite que determinadas estaciones de alta prioridad usen la red con mayor frecuencia. Las tramas Token Ring tienen dos campos que controlan la prioridad: **el campo de prioridad** y el **campo de reserva**.

Sólo las estaciones cuya prioridad es igual o superior al valor de prioridad que posee el token pueden tomar ese token. Una vez que se ha tomado el token y éste se ha convertido en una trama de información, sólo las estaciones cuyo valor de prioridad es superior al de la estación transmisora pueden reservar el token para el siguiente paso en la red. El siguiente token generado incluye la mayor prioridad de la estación que realiza la reserva. Las estaciones que elevan el nivel de prioridad de un token deben restablecer la prioridad anterior una vez que se ha completado la transmisión.

Mecanismos de control

Las redes Token Ring usan varios mecanismos para detectar y compensar los fallos de la red. Uno de estos mecanismos consiste en seleccionar una estación de la red Token Ring como el monitor activo. Esta estación actúa como una fuente centralizada de información de temporización para otras estaciones del anillo y ejecuta varias funciones de mantenimiento del anillo. Potencialmente cualquier estación de la red puede ser la estación de monitor activo.

Una de las funciones de esta estación es la de eliminar del anillo las tramas que circulan continuamente. Cuando un dispositivo transmisor falla, su trama puede seguir circulando en el anillo e impedir que otras estaciones transmitan sus propias tramas; esto puede bloquear la red. El monitor activo puede detectar estas tramas, eliminarlas del anillo y generar un nuevo token.

La topología en estrella de la red Token Ring de IBM también contribuye a la confiabilidad general de la red. Las **MSAU** (unidades de acceso de estación múltiple) activas pueden ver toda la información de una red Token Ring, lo que les permite verificar si existen problemas y, de ser necesario, eliminar estaciones del anillo de forma selectiva.

Otro mecanismo de control de fallos de red es el conocido como **Beaconing**. Cuando una estación detecta la existencia de un problema grave en la red (por ejemplo, un cable roto), envía una **trama de beacon**. La trama de beacon define un dominio de error. Un dominio de error incluye la estación que informa acerca del error, su vecino corriente arriba activo más cercano (NAUN) y todo lo que se encuentra entre ellos.

Entones el beaconing inicia un proceso denominado **autoreconfiguración**, en el que los nodos situados dentro del dominio de error automáticamente ejecutan diagnósticos. Este es un intento de reconfigurar la red alrededor de las áreas en las que hay errores. Físicamente, las MSAU pueden lograrlo a través de la reconfiguración eléctrica.

1.3.3.10.3. Redes LAN DFFI

Las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra) (Figura 1.26), surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

Están implementadas mediante una física de estrella (lo más normal) y lógica de anillo doble de token, uno transmitiendo en el sentido de las agujas del reloj (anillo principal) y el otro en dirección contraria (anillo de respaldo o back up), que ofrece una velocidad de 100 Mbps sobre distancias de hasta 200 metros, soportando hasta 1000 estaciones conectadas. Su uso más normal es como una tecnología de backbone para conectar entre sí redes LAN de cobre o computadores de alta velocidad.

El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de la FDDI se conocen con el nombre de primario y secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.

Se distinguen en una red FDDI dos tipos de estaciones: las estaciones **Clase B, o estaciones de una conexión (SAS)**, se conectan a un anillo, mientras que las de **Clase A, o estaciones de doble conexión (DAS)**, se conectan a ambos anillos.

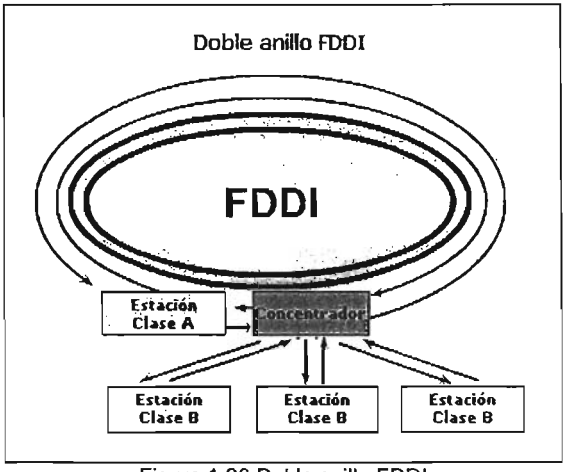


Figura 1.26 Doble anillo FDDI

Las SAS se conectan al anillo primario a través de un concentrador que suministra conexiones para varias SAS. El concentrador garantiza que si se produce una falla o interrupción en el suministro de alimentación en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando se conectan al anillo PC o dispositivos similares que se encienden y se apagan con frecuencia.

Las redes FDDI utilizan un mecanismo de transmisión de tokens similar al de las redes Token Ring, pero además, acepta la asignación en tiempo real del ancho de banda de la red, mediante la definición de dos tipos de tráfico:

1. **Tráfico Síncrono**: Puede consumir una porción del ancho de banda total de 100 Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.
2. **Tráfico Asíncrono**: Se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.

El ancho de banda síncrono se asigna a las estaciones que requieren una capacidad de transmisión continua. Esto resulta útil para transmitir información de voz y vídeo. El ancho de banda restante se utiliza para las transmisiones asíncronas

FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.
El mecanismo de prioridad de la FDDI puede bloquear las estaciones que no pueden usar el ancho de banda síncrono y que tienen una prioridad asíncrona demasiado baja.

En cuanto a la codificación, FDDI no usa el sistema de Manchester, sino que implementa un esquema de codificación denominado **esquema 4B/5B**, en el que se usan 5 bits para codificar 4. Por lo tanto, dieciséis combinaciones son datos, mientras que las otras son para control.

Debido a la longitud potencial del amillo, una estación puede generar una nueva trama inmediatamente después de transmitir otra, en vez de esperar su vuelta, por lo que puede darse el caso de que en el anillo haya varias tramas a la vez.

Las fuentes de señales de los transceptores de la FDDI son LEDs (diodos electroluminiscentes) o lásers. Los primeros se suelen usar para tendidos entre máquinas, mientras que los segundos se usan para tendidos primarios de backbone.

Tramas FDDI

Las tramas en la tecnología FDDI poseen una estructura particular. Cada trama se compone de los siguientes campos:

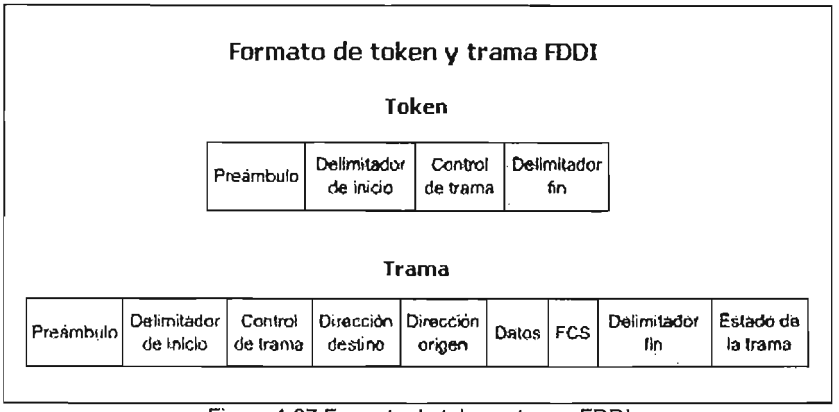


Figura 1.27 Formato de token y trama FDDI

- Preámbulo, que prepara cada estación para recibir la trama entrante.
- Delimitador de inicio, que indica el comienzo de una trama, y está formado por patrones de señalización que lo distinguen del resto de la trama.
- Control de trama, que contiene el tamaño de los campos de dirección, si la trama contiene datos asíncronos o síncronos y otra información de control.
- Dirección destino, que contiene la dirección física (6 bytes) de la máquina destino, pudiendo ser una dirección unicast (singular), multicast (grupal) o broadcast (cada estación).
- Dirección origen, que contiene la dirección física (6 bytes) de la máquina que envió la trama.
- Secuencia de verificación de trama (FCS), campo que completa la estación origen con una verificación por redundancia cíclica calculada (CRC), cuyo valor depende del contenido de la trama. La estación destino vuelve a calcular el valor para determinar si la trama se ha dañado durante el tránsito. La trama se descarta si está dañada.
- Delimitador de fin, que contiene símbolos que indican el fin de la trama.
- Estado de la trama, que permite que la estación origen determine si se ha producido un error y si la estación receptora reconoció y copió la trama

Medios en las redes FDDI

FDDI especifica una LAN de dos anillos de 100 Mbps con transmisión de tokens, que usa un medio de transmisión de fibra óptica.

Aunque funciona a velocidades más altas, FDDI es similar a Token Ring. Ambas configuraciones de red comparten ciertas características, tales como su topología (anillo) y su método de acceso al medio (transferencia de tokens).

Una de las características de FDDI es el uso de la fibra óptica (Figura 1.28), como medio de transmisión. La fibra óptica ofrece varias ventajas con respecto al cableado de cobre tradicional, por ejemplo:

- Seguridad: la fibra no emite señales eléctricas que se pueden interceptar.
- Confiabilidad: la fibra es inmune a la interferencia eléctrica.
- Velocidad: la fibra óptica tiene un potencial de rendimiento mucho mayor que el del cable de cobre.

Figura 1.28 Tipos de Fibra óptica

Existen dos clases de fibra: monomodo (también denominado modo único); y multimodo. La fibra monomodo permite que sólo un modo de luz se propague a través de ella, mientras que la fibra multimodo permite la propagación de múltiples modos de luz. Los **modos** se pueden representar como haces de rayos luminosos que entran a la fibra en un ángulo determinado.

Cuando se propagan múltiples modos de luz a través de la fibra, éstos pueden recorrer diferentes distancias, según su ángulo de entrada. Como resultado, no

llegan a su destino simultáneamente; a este fenómeno se le denomina **dispersión modal**.

La fibra monomodo puede acomodar un mayor ancho de banda y permite el tendido de cables de mayor longitud que la fibra multimodo. Debido a estas características, la fibra monomodo se usa a menudo para la conectividad entre edificios mientras que la fibra multimodo se usa con mayor frecuencia para la conectividad dentro de un edificio. La fibra multimodo usa los LED como dispositivos generadores de luz, mientras que la fibra monomodo generalmente usa láser.

CAPITULO 2. Protocolos de comunicación TCP/IP

2.1. Historia de TCP/IP

Internet es una consecuencia directa de la guerra fría. En los años 60 la rivalidad existente entre Rusia y Estados Unidos, con la posibilidad real de guerra atómica, además de la rivalidad existente en la carrera espacial, llevó al planteamiento por parte del ejército americano del diseño de un sistema de comunicaciones que fuera capaz de sobrevivir a un conflicto.

La solución era una red compuesta por ordenadores en la que todos los nodos tuvieran la misma importancia, de forma que la desaparición de uno de ellos no afectara al tráfico general, ya que cada nodo de la red decidiría qué camino seguirían los datos que llegaran a él. Por último, los datos se dividirían en "paquetes", que podrían seguir rutas diferentes, pero que deberían reunirse finalmente en el punto de destino.

La formulación del concepto había comenzado en 1961 cuando Leonard Kleinrock del MIT presentó un trabajo sobre "conmutación de paquetes". La puesta en marcha fue financiada por el Pentágono a través de su agencia ARPA *(Advanced Research Projects Agency)* , para probar de forma práctica su viabilidad. Posteriormente, pasó a depender del Ministerio de Defensa, pasando a llamarse DARPA *(Defense Advanced Research Projects Agency)*. Durante su fase inicial, ARPA estaba formada por una red de líneas alquiladas, conectadas por nodos de conmutación. La red se denominó ARPAnet y los nodos de conmutación se denominaban IMP *(Internet Messages Processors)*.

En el año 1968, la empresa Bolt, Baranek & Newman (BBN), ganó el contrato para la instalación de la red, por lo que gran parte del desarrollo de Internet y TCP/IP se basó en el trabajo realizado por esta empresa.

En 1969 (año de la llegada del hombre a la Luna), se abrió el primer nodo de la red ARPANET, en UCLA (Universidad de California Los Angeles), el segundo en la Universidad de Stanford, donde trabajaba Douglas Engelbart (que había creado el ratón y trabajaba en hipertexto). Posteriormente se unieron la Universidad de California Santa Bárbara y la Universidad de Utah, funcionando con ordenadores Honeywell 316.

Enseguida comenzó a servir de unir ordenadores a comunicar a personas. En 1969, se crea en UCLA el concepto de RFC. En 1972 apareció el primer programa de correo electrónico.

En 1971 entró en servicio normal. Las máquinas utilizaban ARPAnet mediante la conexión a un IMP y utilizando el protocolo 1822 (del número de documento técnico que describia dicho protocolo). Durante los primeros años hubo un amplio proceso de refinamientos y modificaciones conforme los usuarios solicitaban mas funciones al sistema.

Una de las primeras necesidades que apareció era la posibilidad de transferir ficheros entre máquinas y aceptar registros de entrada remotos. Tras toda una serie de protocolos de prueba, se implementó NCP *(Network Control Program)* que permitía la trasferencia de ficheros y el registro de entrada remoto. Mas adelante a través de FTP, se añadió el correo electrónico, con lo que junto NCP, se formo el núcleo de los servicios básicos de ARPANET.

En el año 1973, se vio que NCP era incapaz de manejar el tráfico y las nuevas posibilidades previstas. Se inició el camino que llevaría al nacimiento de TCP/IP. En un artículo publicado por Cerf y Kahn se describía un sistema que incluía un protocolo de aplicación estandarizado, con confirmación de extremo a extremo. Los rudimentos de TCP/IP y la arquitectura de routers se propusieron por primera vez en 1974.

Ninguno de estos conceptos era realmente novedoso, pero lo realmente importante de la propuesta de Cerf y Kahn, era la sugerencia de que el nuevo protocolo fuese independiente de la red y del hardware existente. También proponían conectividad universal a través de la red. Estas dos ideas eran de una gran radicalidad, ya que en aquel momento todo el software y hardware existente era propietario, ya que permitían que cualquier tipo de plataforma participara en la red. El hecho que el protocolo con estas bases se creó y fue conocido como TCP/IP.

En 1981 se creó una serie de RFC, estandarizándose en la versión 4 de TCP/IP para ARPANET. En 1982 TCP/IP sustituyó a NCP como protocolo dominante de la creciente red. En aquellas fechas la tasa de conexión de máquinas se estimaba en una máquina cada veinte días, lo que representaba un fenomenal crecimiento.

Para coordinar todos los temas relacionados con este entorno, se creó el IAB *(Internet Activities Board)* en 1983. Este grupo es el máximo responsable, a la hora de dictar normas y directrices dentro de este campo. El IAB, está organizado en dos grandes grupos, el IRTF *(Internet Research Task Force)* y el IETF *(Internet Engineering Task Force)*; existen una serie de informes sobre todas las propuestas y desarrollos Internet denominadas "RFCs" *(Request for Comments)*. Estos documentos numerados en orden cronológico, reflejan todas

las investigaciones, medidas y normas que se han desarrollado para "Internet". A esta información, se puede acceder a través de la propia red.

En 1983, el Departamento de Defensa, obligó a que todos los ordenadores conectados a ARPANET utilizasen el TCP/IP y los protocolos relacionados. Para facilitar la adopción de este estándar, se promocionó el desarrollo de esta en la versión del UNIX de Berkeley.

La interconexión de redes se hace a nivel de red y hay dos tendencias claras al igual que en el nivel de transporte:

- Protocolos de la red ARPA:
  - ✓ Internet Protocolo
  - ✓ TCP o UDP
- Protocolos de ISO o ITU:
  - ✓ Protocolo X.75 (que es igual que X.25, pero para la interconexión entre pasarelas).
  - ✓ Normativa ISO X.224 a nivel de transporte.

La meta del protocolo TCP/IP como de cualquier otro es ocultar los detalles hardware de las redes, proporcionando un servicio de comunicaciones universal.

Para realizar la interconexión entre dos sistemas informáticos pertenecientes a distintas redes, tenemos dos opciones:

- Mediante diseño de programas de aplicación.
- Mediante el sistema operativo.

Estas dos opciones tienen unas limitaciones muy fuertes, ya que los programas de aplicación generados para una máquina son muy dependientes de la tecnología que utilice la misma y de la conexión a la red. Es decir, cualquier cambio de la tecnología subyacente del sistema o de la red de comunicaciones, nos obliga a modificar el programa de aplicación. Evidentemente, esta filosofía no sirve.

Deberíamos pues diseñar un sistema que permitiese realizar la interconexión a nivel de red, de forma que los cambios tecnológicos que ocurran por debajo, afecten solamente a ciertos parámetros de los protocolos de interconexión, sin que afecte a los programas de usuario.
Así pues, deberíamos ser capaces de diseñar un sistema que permitiese:

- Ocultar la arquitectura de interconexión a los usuarios.No imponer topologías determinadas.

- Ser independiente del interfase con el usuario. Sobre esta capa el diseñador construye la interfase para que el usuario llame al protocolo (p.e. TCP/IP) para establecer la interconexión.

2.2. El sistema de comunicaciones Internet

El sistema de comunicaciones INTERNET está formado por múltiples redes de paquetes interconectadas entre sí a través de elementos denominados gateways. En el contexto de INTERNET, el término gateway tiene el significado de encaminador (esto lo veremos posteriormente).

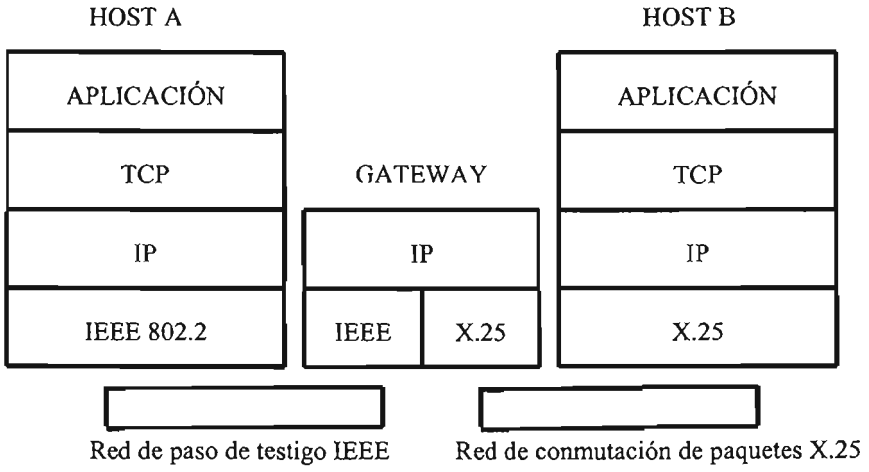


Figura 2.1 Ejemplo de comunicación de dos nodos en una red Internet

En la figura 2.1 el gateway tiene una interfaz con la red de paso de testigo y otro con la red de conmutación de paquetes.

2.2.1. Direcciones Internet o Direcciones IP

Las direcciones Internet son las direcciones que utiliza el protocolo IP para identificar de forma única e inequívoca un nodo u host[1]1 en la Internet. Cada host en la Internet tiene asignada una dirección, la dirección IP que consta de dos partes como indica la figura 2.2.
1

[1] 1 El término host se refiere a un nodo de la red, que en la mayoría de las ocasiones, será un ordenador, pero en otras será, un encaminador.

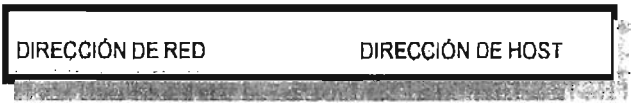


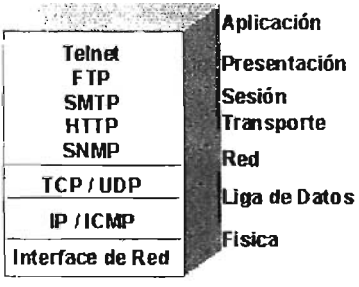
Figura 2.2 Estructuras de las direcciones Internet

Para enviar un datagrama a una dirección IP destino, la dirección IP debe transformarse en una dirección de la red física (por ejemplo, una dirección MAC). Esta transformación algunas veces suele ser bastante simple y basta con aplicar un algoritmo a la dirección IP (de forma análoga a como se realiza en X.25), pero otras veces esta transformación requiere de transmisiones adicionales hacia la red para poder localizar la dirección física del host destino.

2.3. Descripción general de los protocolos TCP/IP

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre cualquier par de ordenadores de cualquier red o fabricante, respetando los protocolos de cada red individual.

La figura 2.3 muestra el modelo general de los protocolos TCP/IP con algunas de las aplicaciones normalizadas que los utilizan.



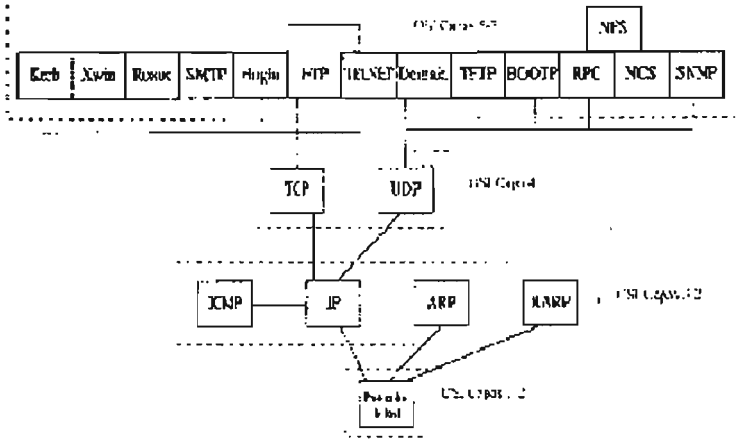


Fig 3. Protocolos y aplicaciones TCP/IP

Figura 2.3 Protocolos y aplicaciones TCP/IP

Los protocolos TCP/IP proporcionan a los usuarios unos servicios de comunicación universales tales como:

- Transferencia de Ficheros
- Login Remoto o Terminal Virtual
- Correo Electrónico
- Acceso a Ficheros Distribuidos
- Administración de Sistemas
- Manejo de Ventanas

En una primera aproximación se podrían estructurar los protocolos TCP/IP en cinco niveles funcionales como muestra la Figura 2.4

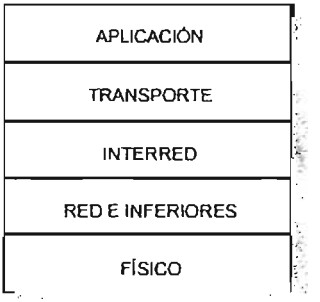


Figura 2.4. Primera aproximación a los niveles TCP/IP

2.3.1. Nivel de Aplicación

En este nivel se encuentran las aplicaciones disponibles para los usuarios. Una aplicación es un proceso de usuario que está cooperando con otro proceso de usuario en una misma máquina o en máquinas diferentes. Ejemplos de tales aplicaciones son el FTP *(File Transfer Protocol)*, y el SMTP *(Simple Mail Transfer Protocol)*.

2.3.2. Nivel de Transporte

El nivel de transporte suministra a las aplicaciones servicios de comunicaciones de extremo a extremo utilizando dos tipos de protocolos: TCP (Protocolo de Control de la Transmisión) fiable y orientado a conexión y el UDP (Protocolo de Datagrama de Usuario) no fiable y no orientado a conexión.

2.3.3. Nivel IP protocolo Internet

El nivel IP se superpone a la red física creando un servicio de red virtual independiente de aquélla. No es fiable ni orientado a conexión. Realiza su mejor esfuerzo para entregar los paquetes denominados datagramas, a su destino. Los datagramas pueden perderse, duplicarse o cambiar de orden de secuencia.

2.3.4. Interfaz de Red

Es la interfaz con la red "real". Puede o no proporcionar fiabilidad en la distribución de datos, que pueden adoptar diferentes formatos. De hecho TCP/IP no especifica ningún protocolo en este nivel, lo que manifiesta la flexibilidad del nivel Internet. Como ejemplos de este interfaz tenemos IEEE 802.2 (para redes de área local), X.25, *Frame Relay* o incluso SNA.

2.3.5. Visión General

La Figura 2.5 muestra los protocolos de cada nivel indicando los datos manejados por cada uno de ellos.

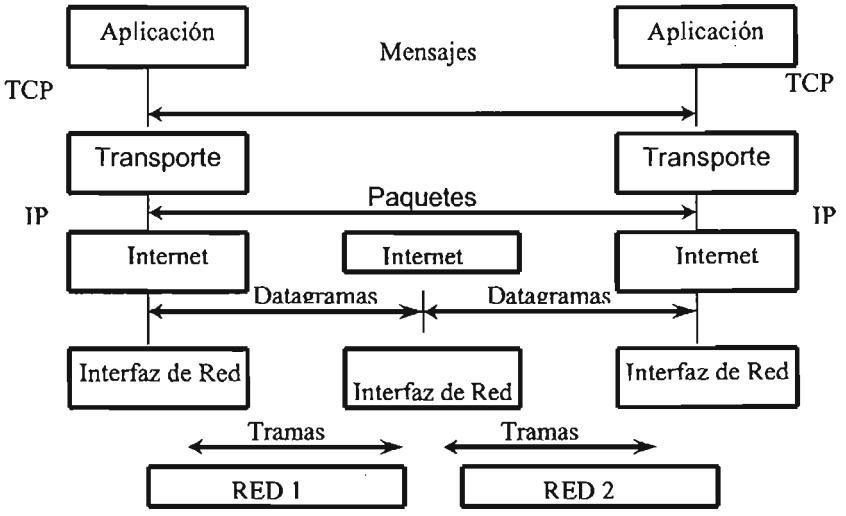


Figura 2.5 Protocolos TCP/IP con sus mensajes

Las aplicaciones se comunican entre sí mediante mensajes. No tiene nivel de presentación. Este nivel debe ser realizado por la aplicación. El nivel de transporte realiza también algunas funciones del nivel de sesión mediante paquetes. El nivel Internet (IP) maneja los niveles de red mediante una interfaz de red. Las unidades de datos intercambiadas en el nivel IP son los datagramas.

2.3.6. TCP/IP y el modelo de referencia OSI

Existen substanciales diferencias entre la concepción del Modelo de Referencia OSI y la del conjunto de protocolos TCP/IP. Históricamente, los protocolos TCP/IP fueron desarrollados antes que el Modelo de Referencia y, al igual que en otras muchas ocasiones, era muy difícil que los promotores y usuarios esperasen a que los comités de ISO completasen sus actividades. Por otra parte TCP/IP tenía que contemplar realidades operativas de sistemas en producción, como la seguridad, la interoperación de redes, la fiabilidad o la gestión de red.

Conceptualmente también existen notables diferencias, como son:

- El concepto de jerarquía en relación al de niveles o capas
- La interoperación de redes
- La fiabilidad extremo a extremo
- Los servicios no orientados a conexión
- La gestión de red

El concepto de jerarquía con relación al concepto de capas es extremadamente sutil y realmente es consecuencia de que en TCP/IP se aplicó posiblemente un mayor grado de pragmatismo que en los trabajos de ISO. En ambas arquitecturas, una tarea de comunicaciones se divide en módulos o entidades que pueden comunicar con entidades pares en otro sistema. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras. Estas entidades deben tener una relación jerárquica, de tal manera que una entidad sólo puede utilizar los servicios de las entidades jerárquicamente inferiores.

Para comunicar entidades pares, TCP/IP da libertad para definir y utilizar múltiples protocolos con funcionalidades distintas. Es decir, en el mismo nivel o capa pueden existir múltiples protocolos, con distinta funcionalidad, dejando libertad al diseñador para la utilización de uno u otro. Lo único que realmente es común a todos los protocolos de un nivel o capa es que comparten el mismo conjunto de protocolos de la capa inferior, es decir, están en una jerarquía superior. Así, en TCP/IP, existen en la capa de transporte, protocolos de

naturaleza bien distinta, como el UDP, no fiable ni orientado a conexión y el TCP, fiable y orientado a conexión. Es opción de los diseñadores de los niveles superiores el utilizar uno u otro. Se dice que el Modelo OSI es más prescriptivo que descriptivo, en el sentido de que dicta los protocolos de un nivel determinado que deben realizar unas funciones determinadas.

Estas diferencias no suponen que haya funciones que se puedan realizar con OSI y no con TCP/IP Lo que sucede es que el conjunto de protocolos TCP/IP, al ser modular y jerárquico, proporciona a los diseñadores mayor grado de libertad. Podría decirse que estas diferencias son consecuencia de cómo se realiza el proceso de generación de normas. En ISO, primero se especifican y posteriormente se realizan implementaciones; en Internet se especifican al tiempo en que se desarrollan, con lo que los ciclos se acortan y además tienen un carácter más orientado a la solución de requisitos reales. La aceptación de facto se consigue, difundiendo por Internet tanto las especificaciones como las implementaciones en documentos denominados RFC, Request for Comments.

Los protocolos TCP/IP se han concebido desde su origen para interconectar sistemas no conectados a la misma red. Las características del protocolo IP emanan de este requisito.

Los protocolos TCP/IP proporcionan una fiabilidad extremo a extremo. El protocolo IP de nivel de red no es fiable, es decir, no garantiza que los paquetes entregados sean correctos y que conserven la secuencia con que han sido emitidos. En otras palabras, IP supone que las redes son relativamente fiables y, en caso necesario, la fiabilidad debe garantizarse por los protocolos de transporte en los sistemas de usuario (TCP).

Por el contrario, X.25, por ejemplo, define un conjunto de protocolos tanto a nivel de enlace como a nivel de red para control de errores como control de flujo, lo que es redundante con funciones similares proporcionadas por otros niveles y disminuye la eficiencia y capacidad de la red.

Como consecuencia de lo anterior, los servicios de IP son no orientados a conexión. En cualquier nivel de TCP/IP, se contempla la posibilidad de un servicio no orientado a conexión o datagrama. La conectividad extremo a extremo debe proporcionarse en los niveles superiores. Es verdad, ciertamente, que OSI también contempla la posibilidad de utilización de datagramas, si bien se suelen considerar como una alternativa a la opción principal.

En los primeros documentos de OSI no se contemplaban las funciones de gestión. Actualmente no es el caso, y es posible que los protocolos y servicios de gestión definidos por ISO alcancen un cierto nivel de aceptación, si bien no son tan populares como los definidos en TCP/IP.

Como consecuencia de todo lo anterior, la situación es que hay muy pocas aplicaciones definidas y realmente utilizadas dentro del modelo de referencia OSI. La más extendida quizás sea posiblemente el sistema de correo electrónico basado en la Recomendación X.400 equivalente a MOTIS de ISO. Sin embargo,

hay un amplio conjunto de aplicaciones TCP/IP que son estándares de facto y muy populares, como TELNET, FTP, X-Window, SMTP, NFS, etc.

2.4. Protocolos del Nivel Internet

Los protocolos más importantes del nivel Internet son los siguientes:

- Protocolo IP (Protocolo Internet)
- Protocolo ICMP (Protocolo de Mensajes de Control Internet)
- Protocolo ARP (Protocolo de Resolución de Direcciones)
- Protocolo RARP (Protocolo Inverso de Resolución de Direcciones)

2.4.1. El protocolo IP

La característica principal es que no es fiable y no está orientado a conexión, lo que significa:

- No garantiza el control de flujo
- No garantiza la recuperación de errores
- No garantiza que los datos lleguen a su destino

El protocolo IP siempre trabaja con entregas de datagramas (sin conexión previa) que viajan de extremo a extremo de la red. Los datagramas enviados por IP pueden perderse, llegar desordenados o duplicados, IP no se responsabiliza de estas situaciones que tendrán que ser contempladas por el nivel TCP No obstante, la red realiza su mejor esfuerzo para intentar que los datagramas IP alcancen su destino.

Este protocolo se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por dónde se deben encaminar los datagramas salientes pudiendo llevar a cabo labores de fragmentación y reensamblado.

2.4.1.1. El mecanismo de direcciones IP

Cada host posee una dirección IP, que es la encargada de identificar la red y el host. Las direcciones IP son siempre direcciones de 32 bits de longitud, representadas por decimales seguidos de un punto.

Ejemplo: 123.003.002.008

Cada dirección IP consta de dos direcciones lógicas:
Dirección IP = <Dirección de la Red> <Dirección del host>

En algunos sistemas también puede identificarse la subred en la que está ubicado el host:

Dirección IP = <Dirección de la Red> <Dirección de la Subred> <Dirección del host>

Esta segunda forma de direccionamiento surge como consecuencia del enorme crecimiento de Internet. El hecho de asignar direcciones IP a los hosts llegó a ser demasiado inflexible a la hora de realizar pequeños cambios en las configuraciones de las redes locales que estaban conectadas a Internet; estos cambios se debian principalmente a que el número de host que estaban conectados a una red llegaba a ser muy grande y había que realizar una división de la red en dos redes o más de menor tamaño. Debido a esto surgió el término Subred, al particionar la red lógica en redes menores. No obstante la subred tiene existencia propia dentro de la red original, pero no respecto al mundo exterior que ve una única red, la Internet. En la figura 2.7 puede observarse el ejemplo de unas redes divididas en múltiples subredes y conectadas entre sí mediante encaminadores, es decir gateways (GW) en terminología Internet.

2.4.1.2. Formatos de las direcciones IP

Existen cinco tipos de formatos diferentes para las direcciones IP que las dividen en las siguientes clases:

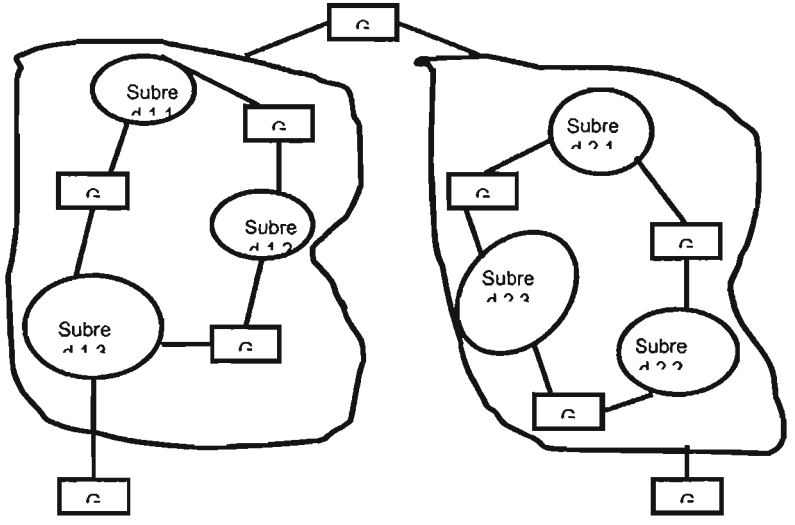
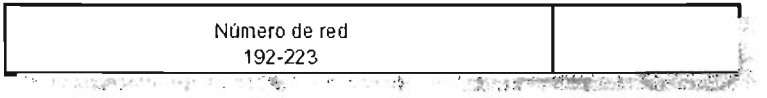


Figura 2.7 Redes divididas en múltiples subredes

CLASE A: Contiene 7 bits para direcciones de red (lo que permite un máximo de 27=128 redes), cada una de las cuales puede tener 224=l6.777.2l6 ordenadores. Se utiliza cuando se tienen muchos hosts.

CLASE B: Tiene 14 bits para direcciones de red y 16 bits para direcciones de host. Esto permite un máximo de 214=16.536 redes de como máximo 216=65.536 hosts por red.

CLASE C: Tiene 21 bits para direcciones de red y 8 bits para direcciones de host. Esto permite un máximo de 221=2.097.l42 redes de 28=256 hosts como máximo cada una.



CLASE D: Se reservan todas las direcciones para multidestino (multicasting), esto es, un ordenador transmite un mensaje a un grupo específico de ordenadores, entre ordenadores de la clase D

CLASE E: Esta clase se utiliza con fines experimentales. Algunos valores de los campos (parte de la dirección correspondiente al host o a la red) están preasignados:

0...0	Se refiere a esta red o a este ordenador local
1...1	Se refiere a todas las redes o a todos los ordenadores
127.0.0.1	Es la dirección de bucle cerrado (loopback). Se refiere siempre a sí misma.

Ejemplo:

126.3.255.255 Significa que es a todos los ordenadores de la red 126.3 (ClaseB)

La desventaja de este esquema de direcciones es que si cambia un ordenador de una red a otra, su dirección IP debe cambiarse también. Además, si varía el tamaño de una red es posible que varíe también la clase de direcciones.

La clase es asignada por el Comité Operativo de la Internet. Lógicamente la clase A (sólo 128 redes) es la más selectiva, por la que se restringe a grandes organismos y corporaciones.

2.4.1.3. Máscara en las direcciones

Una organización que tenga direcciones de red de Clase A o Clase B es muy probable que tenga una red de cierta complejidad constituida por muchas LAN y varios enlaces de WAN. Es conveniente dividir el espacio de estados de forma que coincida con la estructura de la red de acuerdo a una familia de subredes. Para ello, la parte local de la dirección se divide una "parte de subred" y una "parte de sistema", de manera adecuada. El esquema de direcciones IP puede tener problemas de flexibilidad. Considérese, por ejemplo, el caso de la Figura 2.8, que representa el esquema de direcciones de la Universidad de La Laguna

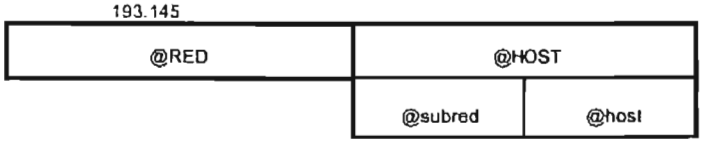


Figura 2.8 Direcciones Internet en la Universidad de la laguna

Si se asignase de una manera fija un octeto para cada subred, el máximo número de nodos por subred sería 255, lo que puede resultar insuficiente. Para conseguir incrementar el número de ordenadores conectados se emplea una máscara en la dirección IP que se aplica a la subred. La máscara es un mecanismo compuesto de "ceros"' y de "unos" mediante el cual los "unos" indican la parte de dirección de red y subred, y los "ceros" se corresponden con las direcciones de host.

Ejemplo: Si tiene una red como la de la ULL, en la que una subred contiene 600 hosts esto significa que serían necesarios 10 bits para poder direccionar todos los hosts que contiene esa subred. Una máscara válida para este caso sería la que muestra la Figura 2.9.

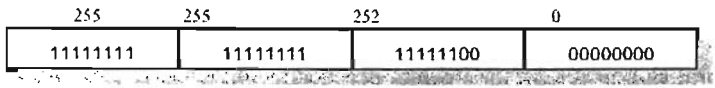


Figura 2.9 Ejemplo de máscara para una subred que necesita 10 bits para direcciones de host

El tamaño de la parte de subred de una dirección y la asignación de números a subredes es responsabilidad de la organización que "posee" esa parte del espacio de direcciones.

2.4.1.3.1. Máscaras de las subredes

El tráfico se encamina hacia un host consultando las partes de red y subred de una dirección de IP. La parte de red de una dirección de Clase A, B, o C tiene un tamaño fijo. Pero las organizaciones pueden decidir sus propios tamaños de subred, por lo que ¿cómo pueden reconocer los encaminadores estos campos?. La respuesta es que hay que configurar los sistemas para que conozcan el tamaño de la parte de subred de la dirección.

El tamaño del campo de subred se almacena realmente en un parámetro de configuración llamado máscara de subred.. La máscara de subred es una secuencia de 32 bits. Los bits que corresponden a los campos de red y subred de una dirección se ponen a 1 y los bits para el campo del sistema se ponen a 0.

Por ejemplo, si se usa el tercer byte de las direcciones que empiezan por 128.121 para identificar las subredes, la máscara es:

11111111 11111111 11111111 00000000

Normalmente las máscaras de subred se expresan en notación decimal con puntos. La máscara anterior se puede escribir: 255.255.255.0
A veces la máscara se escribe en hexadecimal, como: FF-FF-FF-00

Los host y encarninadores conectados a una subred se configuran con la máscara de la subred. Se suele usar una única máscara de subred en toda una internet de organización. Hay excepciones a esta práctica, y algunas organizaciones usan varios tamaños diferentes de subred.

Por ejemplo, si una red tiene muchas líneas punto a punto, no seria adecuado usar los números de subred ya que sólo hay dos sistemas en cada subred punto a punto. Una organización podría decidir usar máscaras de 14 bits (255.255.255.252) para sus líneas punto a punto.

2.4.1.4. Los datagramas IP

Los datagramas IP contienen una cabecera con información para el nivel IP y datos. Los datagramas se encapsulan en tramas, que dependiendo de la red física utilizada tienen una longitud determinada. Por ejemplo, en Ethernet, la longitud máxima es de 1500 bytes. El formato de la cabecera se puede observar en la figura 2.10

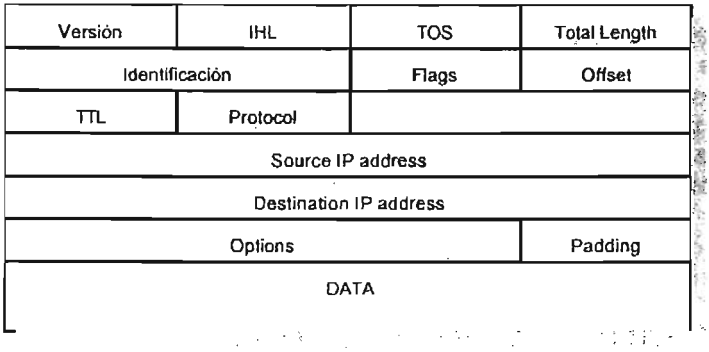


Figura 2.10 Cabecera de datagramas IP

Los campos de que consta la cabecera IP son los siguientes:

- **Versión**: Es la versión del Protocolo IP. La versión actual es la 4.
- **IHL**: Longitud de la cabecera IP en palabras de 32 bits.
- **TOS**: Tipo de Servicio. Indica las prioridades deseadas. Está compuesto por dos subcampos:
  - ✓ Los cinco bits siguientes indican el tipo de servicio. Normalmente no se utilizan, pero algunas aplicaciones como el control de encaminamiento y los algoritmos de colas en las pasarelas utilizan este campo.
- Total Length: Longitud total del datagrama (cabecera y datos) expresada en bytes.
- **Identificación:** A todos los fragmentos en que se puede dividir un datagrama se les asigna el mismo identificador. Contiene un entero que identifica el datagrama. Cuando se produce una fragmentación de un datagrama, el campo del identificador se copia en todos los datagramas ya fraccionados. De esta manera, el receptor puede identificar los datagramas que componen el datagrama fragmentado.
- **Flags**: Son identificadores de control:
  - ✓ Reservado
  - ✓ Se permite/no fragmentación
  - ✓ Ultimo fragmento/más fragmentos

- **Fragment Offset**: Se utiliza en el reensamblaje de los datagramas previamente segmentados. Especifica la posición *(offset)* en bytes de cada fragmento del datagrama original. El campo de offset se va incrementando en cada fragmento del datagrama que se envía empezando con cero.
- **TTL**: Time to live. Tiempo de vida del datagrama. Especifica en segundos el tiempo que puede viajar por una red un datagrama. El tiempo de vida está limitado a 255 segundos. Cada vez que un datagrama pasa a través de un encaminador, el encaminador resta de este campo el tiempo que tarda en procesar el datagrama (1 como mínimo, aunque el tiempo de proceso sea menor). Cuando este campo alcanza el valor cero antes de alcanzar su destino, se supone que el datagrama está perdido en un bucle cerrado y se descarta.
- **Protocol**: Indica el protocolo de nivel superior para el cual el nivel IP está realizando el servicio de transporte de datos en el datagrama. Especifica el formato del área de datos. Como ejemplos de protocolos superiores están los siguientes:
  - ✓ 1 ICMP
  - ✓ 6 TCP
  - ✓ 5 EGP
  - ✓ 9 IGP
  - ✓ 17 UDP
  - ✓ 29 ISO-TP4
- **Checksum**: Son unos bytes de verificación que afectan a la cabecera y no a los datos. El checksum se calcula como el complemento a uno de la suma (en complemento a uno) de todos los bits que componen la cabecera. Normalmente hay que recalcular el checksum de cada nodo por el que pasa el datagrama ya que, al ir atravesando los distintos gateways, el campo TTL (tiempo de vida) va variando.
- **Source IP Address**: Dirección IP del host origen.
- **Destination IP Address**: Dirección IP del host destino.
- **Options**: Una implementación IP no está obligada a generar diversas opciones para los datagramas que ella misma crea pero lo que sí debe hacer es procesar los datagramas que la contengan. Ejemplos de opciones son:
  - ✓ *Opción de Seguridad*: Utilizada por aplicaciones seguras.
  - ✓ *Opción de Ruta Prefijada*: En el campo Options se especifica una lista de direcciones Internet que componen el camino que deberá seguir el datagrama.
  - ✓ *Opción de Registrar la Ruta*: El host fuente crea una lista vacía de direcciones Internet en el campo Options y cada máquina que manipula el datagrama ha de grabar su dirección en esta lista.

- ✓ *Opción de Registrar la Hora*: Es similar a la opción anterior. Cada máquina graba la hora en la que manipuló el datagrama y opcionalmente graba también su dirección.

- **Padding**: Son bits de relleno. Cuando se utilizan opciones en el campo Options los datagramas se rellenan con bits a cero, para ajuste a frontera de 4 octetos.
- **Data**: Son los datos contenidos en el datagrama que pasan al protocolo superior indicado en el campo Protocol. Por definición, el tamaño máximo de un datagrama IP es de 65535 bytes y, suponiendo que la longitud de la cabecera IP es de 20 bytes, quedan 65515 bytes para datos.

2.4.1.5. Fragmentación y reensamblado en el protocolo IP

Cuando los datagramas IP viajan de unos equipos a otros pueden atravesar diferentes redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño se le denomina MTU (Unidad Máxima de Transmisión). Una red no puede transmitir ningún paquete cuya longitud exceda la del MTU de dicha red. Por ejemplo, en Ethernet, los paquetes no pueden superar los 1.500 bytes.

Debido a esto es necesario algún mecanismo que permita reconvertir los datagramas IP en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina fragmentación y reensamblado.

La fragmentación divide los paquetes en varios fragmentos de menor longitud, mientras que el reensamblado realiza el proceso inverso.

Si se emplea el concepto "nivel", la fragmentación se realiza en el nivel más inferior posible de forma transparente al resto de los niveles Cuando el nivel IP fragmenta un datagrama, el nivel TCP no tiene conocimiento de ello.

El nivel IP es el encargado de fragmentar y reensamblar. En la fragmentación, el mecanismo es el siguiente:

- **Paso 1**: Se comprueba si el indicador de DF (del campo Flags de la cabecera IP) permite fragmentación, en cuyo caso se sigue con el Paso 2.
- **Paso 2**: Se comprueba si el campo Data (Datos) se puede dividir en dos o más partes, cada una de las cuales deberá tener una longitud que sea múltiplo de 8. Ir al Paso 3.
- **Paso 3**: Todas estas partes en las que se ha dividido el campo Datos se colocan en formato de datagramas IP, cuya cabecera será una copia de la cabecera original con las siguientes modificaciones:

- El Host asigna a cada fragmento un número de identificación que es el mismo para todos los fragmentos que componen el mismo datagrama.
- El bit de "Más Fragmentos" se inicia a 1 en todos y cada uno de los fragmentos excepto en el último que se pone a 0.
- El campo "Offset" de cada fragmento se inicia al lugar ocupado por cada fragmento de datos en el datagrama original no fragmentado.
- Si hay opciones en el datagrama original, un indicador muestra si el campo de opción debe ser copiado cuando el datagrama es fragmentado. Las opciones de Ruta Prefijada deben copiarse por defecto en todos los fragmentos.
- Cambia el Checksum.

En el host destino se produce el proceso de Reensamblado mediante el cual los fragmentos se unen para formar el fragmento original. Para realizar el reensamblado, el host destino arranca un temporizador iniciándolo al valor del TTL de la cabecera IP y va guardando en un buffer los fragmentos que le van llegando. Cuando vence el temporizador, si no han llegado al destino todos y cada uno de los fragmentos del datagrama original se descarta el datagrama. En el caso de que lleguen todos antes de que venza el temporizador, se copian los datos en un buffer en el lugar que indica el campo FOCET de cada fragmento, obteniéndose de nuevo el datagrama original.

2.4.2. El protocolo ICMP

El protocolo IP se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

En ocasiones, el host destino y los encaminadores necesitan comunicarse con el host fuente, por ejemplo, para que les informe de los errores encontrados al procesar los datagramas. Para esta función y para otras de información de errores o de control se utiliza el protocolo ICMP (*Internet Control Message Protocol*). ICMP se emplea sólo para los fines expuestos, pero no para hacer fiable el protocolo IP. Los datagramas pueden no ser entregados sin ningún tipo de notificación. La fiabilidad debe ser proporcionada por los niveles superiores que utilicen IP.

El objetivo principal del protocolo ICMP (Protocolo de Mensajes de Control de Internet) es proporcionar la información de error o control entre nodos. La implementación del protocolo ICMP es obligatoria como un subconjunto lógico del protocolo IP.

Los mensajes de este protocolo normalmente los genera y los procesa el software TCP/IP de la red y no el usuario. Por ello no es necesario ningún número de puerto en la cabecera del mensaje ICMP
para indicar hacia dónde se dirigen los mensajes.

Una de las utilidades de diagnóstico que lo utilizan es la utilidad ping de UNIX. Esta utilidad sirve para diagnosticar si un ordenador está conectado a la red.

2.4.2.1. Mensajes ICMP

Estos mensajes se envían encapsulados en datagramas IP. El protocolo IP considera como datos los mensajes ICMP. Como se ha visto en apartados anteriores, los datagramas IP se componen de una cabecera IP y del campo Datos, que en este caso consta de una cabecera ICMP y de un campo datos como muestra la Figura 2.11

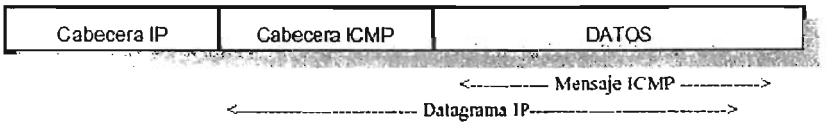


Figura 2.11 Encapsulación del mensaje ICMP

La estructura del mensaje ICMP se muestra en la Figura 2.12

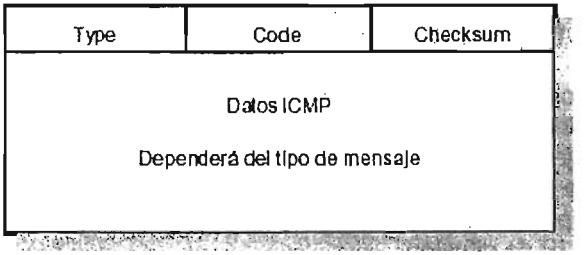


Figura 2.12 Formato del mensaje ICMP

- **Type**: Especifica el tipo de mensaje. Los tipos se expondrán en el apartado siguiente.
- **Code**: Contiene el código del error que afecta al datagrama al que se refiere el mensaje IP..

- **Datos ICMP**: Normalmente el campo datos contiene una parte del mensaje IP original (mensaje causante de generar el mensaje ICMP).

2.4.2.1.1. Tipos de Mensajes ICMP

Existen los siguientes tipos:

- **Mensajes de Destino no Alcanzable**: Estos mensajes los utilizan los encaminadores y en algunas ocasiones los host destino. En un encaminador este mensaje se envía (de acuerdo con las tablas de encaminamiento del encaminador) cuando la distancia a la red es infinita o cuando el encaminador no puede enviar el datagrama a la red destino por cualquier motivo. Un host envía este mensaje si el protocolo de nivel superior o el puerto especificado no se encuentran en estado activo en el host.
- **Mensajes de Control de Congestión**: Cuando un host destino tiene los buffers llenos, envía este mensaje al host origen indicándole este suceso. Este envío suele producirse antes de que el buffer se llene al 80% para que el emisor ralentice los mensajes.
- **Mensajes de Redireccionamiento**: Estos mensajes los envían los encaminadores al host emisor. Indican si el datagrama IP se enviará a través de otro encaminador diferente. La nueva ruta será más óptima.
- **Mensaje de Tiempo Excedido**: Es el mensaje que se envían los encaminadores cuando el campo TTL del datagrama IP es cero, o si el temporizador de reensamblado expira antes de que se hayan recibido todos los fragmentos del datagrama inicial.

Estos cuatro tipos de mensajes se denominan Mensajes de Error.
Existen determinadas circunstancias en las cuales no deben generarse esta clase de mensajes:

- Para responder a otro mensaje de error ICMP
- Para responder a un datagrama IP cuya dirección de destino es una dirección IP de difusión.

- **Mensajes de Petición/Respuesta de Eco**: Son mensajes que utilizan los host para comprobar que el enlace funciona correctamente (mensaje que envía la aplicación ping).

2.4.3. EL protocolo ARP

El Protocolo de Resolución de Direcciones, ARP (Address Resolution Protocol) es un protocolo que se utiliza para convertir las direcciones IP en direcciones de

la red física (por ejemplo, direcciones MAC). Las especificaciones de ARP están descritas en la RFC 826.

Los protocolos TCP/IP direccionan los distintos hosts de la Internet mediante direcciones IP, pero al intentar enviar un datagrama a su destino (p. ej.: 128.3.4.7), es necesario encontrar la dirección de la red física. Por ello, en cada host existe un módulo ARP cuya misión es convertir las direcciones IP en direcciones físicas que puedan entender los manejadores. Para poder realizar esta conversión, este módulo utiliza una tabla, denominada Tabla de Direcciones ARP, que la mayoría de los ordenadores trata como si fuera una memoria intermedia ("caché"), de forma que la información que lleva mucho tiempo sin utilizarse se borra. Así, por ejemplo, en 4.3 BSD la memoria intermedia se refresca cada 20 minutos.

Cuando se envía un datagrama IP a un host destino, el módulo ARP busca en la Tabla de Direcciones la correspondencia entre la dirección IP y la dirección física. Si existe la entrada en la tabla se procede a la transmisión.

Si, por el contrario, la dirección IP del host destino no se encuentra en la tabla de direcciones, se genera una petición ARP que se difunde a través de toda la red. El paquete que engloba esta petición se compone, entre otros, de los campos que muestra la Figura 2.13

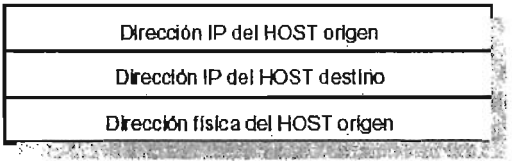


Figura 2.13 Petición ARP

Si alguna de las máquinas de la red reconoce su propia dirección IP en el paquete de petición, envía un mensaje de respuesta al host origen. A su vez, la respuesta se compone de los campos que muestra la Figura 2.14

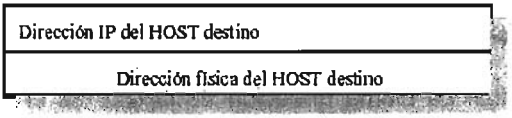


Figura 2.14 Respuesta ARP

La dirección física del host destino se introduce a continuación en la tabla de direcciones del host origen.

2.4.4. El protocolo RARP

El Protocolo Inverso de Resolución de Direcciones RARP (Reverse Address Resolution Protocol), se utiliza cuando, al producirse el arranque inicial, los host no conocen su dirección IP. Es un mecanismo similar al mecanismo ARP con la diferencia de que la dirección física de cada host, en el caso de RARP es un parámetro conocido, mientras que la dirección IP es desconocida.

El protocolo RARP al igual que el protocolo ARP se utiliza en redes de difusión (broadcast). Requiere que existan en la red uno o varios servidores RARP. El formato de los paquetes en este protocolo es el mismo que en ARP. Cuando un host desea conocer su dirección IP envía un paquete, difundiéndolo por la red, que contiene su propia dirección física. Los servidores de RARP al recibir esta información, buscan en la tabla RARP la dirección de red (dirección IP) correspondiente a la dirección física inicial indicada en el paquete, y al encontrarla envían un paquete al host origen con esta información.

Así como el protocolo ARP se incorpora normalmente en los productos TCP/IP, el protocolo RARP sólo se incorpora en un número reducido de productos. Se utiliza algún tipo de terminales X, si bien su uso es cada vez menos frecuente.

2.4.5. Principales servicios de IP

Vamos a dar una visión general de los principales servicios de IP. Los fabricantes suministran diferentes productos para IP, y puede que algunos no soporten todas las características que se describen a continuación.

2.4.5.1. Encaminamiento de origen de IP

IP utiliza como parte de su algoritmo de encaminamiento un mecanismo denominado *encaminamiento de origen.* El encaminamiento de origen permite que un protocolo de nivel superior (ULP) determine la forma en que las pasarelas IP encaminan el datagrama. El ULP tiene la opción de pasar una lista de direcciones interred al módulo de IP. Esta lista contiene los nodos IP intermedios que se van a atravesar durante el encaminamiento del datagrama hasta su destino final. La última dirección de la lista es el destino final de un nodo intermedio.Cuando IP recibe un datagrama, utiliza la dirección del campo de encaminamiento de origen para determinar el siguiente salto intermedio. IP utiliza un campo puntero para averiguar la siguiente dirección IP. Si la comprobación del puntero y de los campos de longitud indican que la lista se ha completado, el campo de dirección IP de destino se utiliza para encaminamiento.

El módulo de IP reemplaza entonces el valor de la lista de encaminamiento de origen con su propia dirección. Por supuesto, hay que incrementar el puntero en el valor de una dirección (4 bytes) para que en el siguiente salto se pueda recuperar la siguiente dirección de IP de la ruta. Con esta solución, el datagrama sigue la lista de origen dictada por el ULP y almacena también la ruta durante el camino.

Operaciones de encaminamiento. La pasarela de IP toma decisiones de encaminamiento basándose en la lista de encaminamiento. Si el ordenador de destino reside en otra red, la pasarela debe decidir la ruta de encaminamiento hacia la otra red. Realmente, si el proceso de comunicación implica varios saltos, hay que atravesar cada pasarela, y las pasarelas deben tomar decisiones sobre el encaminamiento.

En cada pasarela se mantiene una tabla de rutas que contiene la siguiente pasarela a atravesar en el camino hacia la red de destino. Dicha tabla contiene una entrada por cada red alcanzable. Dichas tablas pueden ser estáticas o dinámicas, aunque lo más normal es que sean dinámicas. El módulo de IP realiza las decisiones de encaminamiento de todos los datagramas que recibe.

La tabla de rutas contiene una dirección de IP por cada red alcanzable y la dirección de una pasarela vecina (es decir, una pasarela directamente conectada a esta red). La pasarela vecina es la ruta más corta hacia la red de destino. En otro caso, la lógica de la pasarela de IP establece que la pasarela está directamente conectada a esta red.

El encaminamiento de IP se basa en un concepto denominado *métrica de distancia.* Este valor generalmente no es nada más que el número mínimo de saltos entre la pasarela y el destino final. La pasarela consulta su tabla de encaminamiento e intenta encontrar una dirección de red de destino (contenida en la cabecera) igual a una entrada de red contenida en la tabla de encamina miento. Si no se encuentra, se descarta el datagrama y se forma un mensaje de error que se devuelve a la fuente de IP (lo hace un protocolo adjunto a IP, denominado Protocolo de Mensajes de Control de Internet [ICMP]). El mensaje contiene un código de "destino inalcanzable". Si se encuentra una dirección igual en la tabla de encaminamiento, la pasarela lo utiliza para determinar el puerto de salida.

Encaminamiento relajado y estricto. IP proporciona dos opciones para el encaminamiento de los datagramas hasta su destino final. El *encaminamiento relajado de origen* deja a los módulos de IP libertad para escoger los saltos intermedios que se deben realizar para alcanzar las direcciones obtenidas en la lista de fuentes. En cambio, el *encaminamiento estricto de origen* exige que los

datagramas viajen sólo por las redes cuyas direcciones están indicadas en la lista de fuentes. Si no se puede seguir una ruta estricta de fuentes, el IP del ordenador original recibe un mensaje de error. Ambos tipos de encaminamiento requieren que exista la característica de grabación de ruta, de la que hablaremos seguidamente.

2.4.5.2. Opción de grabación de ruta

La opción de grabación de ruta funciona de la misma forma que el encaminamiento de origen con la característica de grabación que acabamos de ver. Esto quiere decir que cualquier módulo de IP que reciba un datagrama debe añadir su dirección a una lista de grabación de ruta. Para que se lleve a cabo la operación de grabación de ruta, el módulo de IP receptor utiliza los campos de longitud y de puntero para determinar si hay espacio suficiente para grabar la ruta. Si la lista de grabación de ruta estuviera llena, el módulo de IP simplemente envía el datagrama sin insertar su dirección. Si no estuviera llena, el puntero se utiliza para encontrar el primer intervalo de octeto libre. Se inserta la dirección y el módulo de IP incrementa el puntero hasta el siguiente intervalo de IP.

2.4.5.3. Opción de marca temporal

Otra opción muy útil de IP es la posibilidad de incluir marcas temporales en los datagramas cuando atraviesan cada módulo de IP de la interred. De esta forma, el gestor de red no sólo puede determinar la ruta del datagrama sino también el instante en el que cada módulo de IP procesó el datagrama. Esto es muy útil para comprobar la eficacia de las pasarelas y de los algoritmos de encaminamiento.

La marca temporal se basa en milisegundos (ms) de la hora universal (hora de Greenwich). Lógicamente, el uso de la hora universal no garantiza absolutamente que las marcas temporales sean completamente exactas, ya que los relojes de cada máquina pueden diferir ligeramente. No obstante, en la mayoría de las redes, el uso de la hora universal en milisegundos proporciona un grado de precisión razonable.

2.4.6. Protocolos del Nivel de transporte

2.4.6.1 El protocolo TCP

2.4.6.1.1 Características del protocolo TCP

TCP es un protocolo orientado a conexión que utiliza los servicios del nivel IP. Al igual que en todo protocolo orientado a conexión, ésta consta de tres fases:

- Establecimiento de la conexión
- Transferencia de datos
- Liberación de la conexión

TCP permite multiplexación, esto es, la capacidad de que una conexión TCP pueda ser utilizada simultáneamente por varios usuarios.

La unidad de datos que maneja TCP se denomina segmento y la longitud de un segmento se mide en caracteres (octetos).

Los canales de comunicación establecidos mediante TCP son dúplex (aunque el enlace sea semidúplex) y se mantiene la secuencia de entrega de datos transferidos.

La transmisión que ofrece TCP es fiable, permite la recuperación ante datos perdidos, erróneos o duplicados y garantiza la secuencia de entrega, para lo que se asigna al segmento de datos un número de secuencia (información de control) y un *checksum* (código de control). La fiabilidad de la transmisión se consigue mediante tres mecanismos diferentes:

- Confirmación de recepción
- Temporizadores de espera de confirmación
- Retransmisión de segmentos

Para disponer de control de flujo, el receptor mantiene una ventana que indica al emisor la cantidad de datos que puede enviar a partir de cada confirmación recibida.

2.4.6.1.2 Conceptos previos

2.4.6.1.2.1. Puertos

Lo más normal es que en un momento dado haya más de un proceso de usuario o aplicación utilizando TCP simultáneamente. Por ello es necesario un método que identifique los datos asociados a cada proceso. Un puerto es una palabra de 16 bits que identifica hacia qué aplicación o proceso deben dirigirse los datos. Se trata de un mecanismo a través del cual las distintas aplicaciones contactan con TCP/IP.

2.4.6.1.2.2. Sockets ó Zócalos

Es un par de números que identifica de manera única cada aplicación. Cada *socket* se compone de dos campos:

1 dirección IP del *host* en el que la aplicación está corriendo.
2 Puerto a través del cual la aplicación se comunica con TCP/IP. Este número de puerto identifica el proceso.

Existen algunas aplicaciones que realizan la función de servidores normalizados que utilizan los servicios TCP/IP, como son TELNET para conexión remota, o FTP para transferencia de ficheros. Por ello, en todas las realizaciones TCP/IP, estas aplicaciones tienen siempre asignado el mismo número de puerto, concretamente la aplicación de transferencia de ficheros FTP tiene asignado el puerto 21 para control y el puerto 20 para datos y TELNET tiene el 23. Estos puertos reservados se denominan "puertos conocidos" *(well_known ports)* y, no deben utilizarlos otras aplicaciones que no sean las previamente asignadas (Telnet, SMTP,. ...). Los números entre el 1 y 255 (ambos inclusive) corresponden a puertos conocidos.

En el entorno UNIX estas asignaciones de puertos se encuentran ubicadas en el fichero "/etc/services". En él se encuentran los puertos bien conocidos, así como puertos para aplicaciones desarrolladas con TCP/IP (como la denominada *sgenserv).* En este fichero también se especifica el protocolo del nivel de transporte que se va a utilizar (TCP o UDP que será analizado posteriormente)

NOTA: SE PUEDE PONER COMO ANEXO

```
# Network services, Internet style
#
tcpmux          1/tcp       #rfc-1078
echo            7/udp
echo            7/tcp
discard         9/udp       #sink null
discard         9/tcp       #sink null
systat          11/tcp
daytime         13/udp
daytime         13/tcp
netstat         14/tcp
chargen         19/udp      generator # character generator
chargen         19/udp                # character generator
ftp-data        20/tcp
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp      mail
time            37/udp      timserver
time            37/tcp      nameserver
name            42/tcp      nameserver
whois           43/tcp      nicname
 mtp            57/tcp      # deprecated
hostnames       101/tcp     #usually from sri-nic
                hostname
snmp            161/udp     # snmp agent query port
snmp-trap       162/udp     # snmp manager trap port
#
# Host specific functions
#
tftp            69/udp
rje             77/top
finger          79/top
link            87/top ttylink
supdup          95/top
ingreslock      1424/tcp
#
# UNIX specitic services
```

Falta parte de la tabla

En la Figura 2.16 se muestran dos procesos comunicados mediante *sockets*.

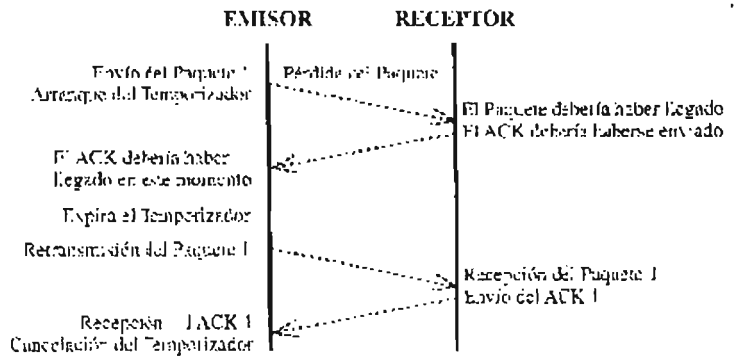


Fig. 24. Mecanismo de parada y espera

Figura 2.15 Mecanismos de parada y espera

2.4.6.1.3 El mecanismo de ventanas deslizantes de TCP

En su versión más elemental, un protocolo de transporte simple utiliza como control de flujo el mecanismo de "Parada y Espera". Un ejemplo de esto puede observarse en la Figura 2.15, en la que se envía un paquete y es recibido correctamente por el receptor, por lo que envía un ACK. En el envío del siguiente paquete éste se pierde y al vencerse el temporizador sin recibir respuesta, el emisor lo retransmite. El envío del siguiente paquete también se realiza de manera correcta.

Con este protocolo el emisor siempre espera un ACK (confirmación) de que el segmento (tratándose de TCP) ha llegado bien por parte del receptor. Ahora bien, este mecanismo desaprovecha gran parte del ancho de banda de la red. Por esta razón, el protocolo TCP utiliza un mecanismo de ventanas para controlar el flujo de la información.

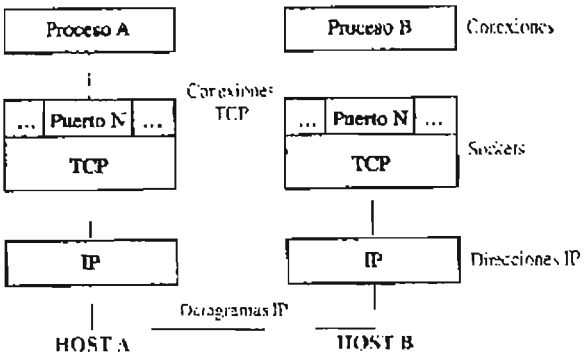


Fig. 23. Comunicación mediante sockets

Figura 2.16 Comunicación mediante Sockets

La idea del mecanismo de ventana deslizante es que el emisor pueda transmitir tantos paquetes de información sin recibir la confirmación de recepción como tenga en la ventana. El rendimiento de este mecanismo depende del tamaño de la ventana y de la velocidad a la que la red transmite los paquetes. Si el tamaño de la ventana es 1 el rendimiento es el mismo que con el mecanismo de parada y espera.

TCP divide las series de caracteres en segmentos y la longitud de cada segmento se mide en caracteres. Así pues, como muestra la Figura 2.17, se pueden distinguir cuatro áreas en el *buffer,* donde:

1) Incluye los caracteres transmitidos y confirmados
2) Incluye los caracteres enviados y no confirmados
3) Incluye los caracteres no enviados pero que pueden enviarse sin esperar a recibir confirmación
4) Incluye los caracteres que no pueden enviarse en ese instante.

Tamaño de la Ventana = Tamaño (B) + Tamaño ©

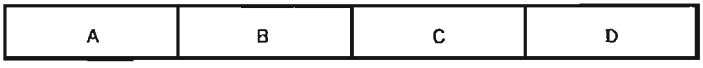


Figura 2.17 Área del buffer

2.4.6.1.4 Reconocimiento y retransmisión de segmentos

Supóngase que el protocolo TCP transmite segmentos de 500 caracteres, que el tamaño de la ventana es de 1.500 caracteres y que existe una comunicación previamente establecida entre dos nodos A y B. Además, se va a producir una secuencia de error con el segundo segmento porque se supone que se va a perder. El diagrama de segmentos transmitidos sería el que muestra la Figura2.18

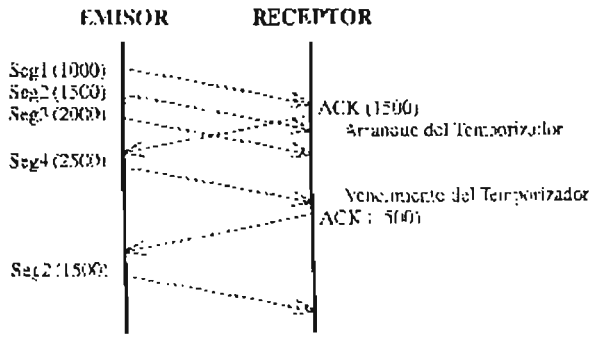


Fig. 26. Transmisión de segmentos con TCP

Figura 2.18 Transmisión de segmentos con TCP

El emisor envía el segmento 1 que contiene desde el carácter 1000 al 1499 (50 caracteres). El receptor recibe correctamente el segmento 1 y envía una confirmación diciendo que el siguiente carácter que espera recibir es el 1500. Mientras tanto, el emisor envía el segmento 2 porque la ventana tiene un tamaño 3 (1500/500=3); el segmento 2 se pierde, pero el emisor sigue transmitiendo su tercer segmento. Tras transmitir el segmento 3, llega la confirmación del segmento 1, por lo que desliza 1 ventana y envía el segmento 4.

Cuando un receptor envía un segmento ACK, arranca un temporizador, de manera que, si al vencer el temporizador no ha recibido el segmento esperado, vuelve a enviar el mismo segmento ACK.

En el ejemplo de la Figura 2.18, al vencer el temporizador del receptor y volver a enviar el segmento ACK(1500) por segunda vez, el emisor se da cuenta de que algo extraño ha ocurrido con el segmento 2 y lo retransmite.

Es importante resaltar que, debido a que TCP mantiene conexiones dúplex, se produce comunicación en ambos sentidos. La transferencia en cada sentido es

independiente. Por ello, el software TCP mantiene dos ventanas por conexión, una se desliza según se van enviando los datos y la otra se desliza según se van recibiendo.

Una de las diferencias entre un simple protocolo de ventana deslizante y el que maneja TCP es que TCP permite que el tamaño de la ventana varíe en el tiempo. Cada confirmación, que contiene el número de caracteres que han sido recibidos, contiene un aviso de cuántos caracteres está preparado para recibir.

La ventaja del mecanismo de variación del tamaño de la ventana es que optimiza el control de flujo. Si el *buffer* de recepción se llena, el receptor no puede recibir más paquetes. En el caso extremo, el receptor avisa de que el tamaño de su ventana es cero para parar toda transmisión. Posteriormente, cuando tiene espacio disponible en el *buffer,* avisa de que el tamaño de su ventana ya no es cero, con lo cual se reanuda el flujo de datos.
Un mecanismo eficaz de control de flujo es esencial en un entorno Internet, debido principalmente a la conexión de ordenadores con distintas velocidades de procesamiento (además de encaminadores y puentes de distintas características). Existen dos problemas fundamentales en el control de flujo:

1) Control de flujo extremo a extremo entre el emisor y el receptor. Por ejemplo, cuando un minicomputador se comunica con un ordenador de gran potencia *(mainframe)* es necesario regular el flujo de entrada o el software del protocolo se sobrecargaría. Por ello, TCP debe implementar un control de flujo extremo a extremo.
2) Los protocolos Internet necesitan un mecanismo de control de flujo que permita la existencia de sistemas intermedios (como pasarelas) para controlar que un emisor emita más tráfico de lo que la máquina pueda tolerar.

Cuando se sobrecargan estos sistemas intermedios (como pasarelas, puentes o encaminadores) se produce lo que se denomina congestión, TCP emplea el esquema de la ventana deslizante para solucionar el problema del control de flujo extremo a extremo, pero no hay un mecanismo explícito para el control de congestión. Sin embargo, una buena implementación de TCP puede detectar y corregir una congestión., no obstante, una mala implementación puede no hacerlo o empeorar el problema. Un esquema de retransmisión cuidadosamente estudiado puede evitar la congestión, mientras que uno no
tan depurado puede agravar este problema.

2.4.6.1.5 Formatos de los segmentos TCP

En la Figura 2.19 se muestra el formato de los segmentos TCP Cada segmento está dividido en dos partes: una cabecera seguida de datos. La cabecera TCP contiene la información de identificación y control.

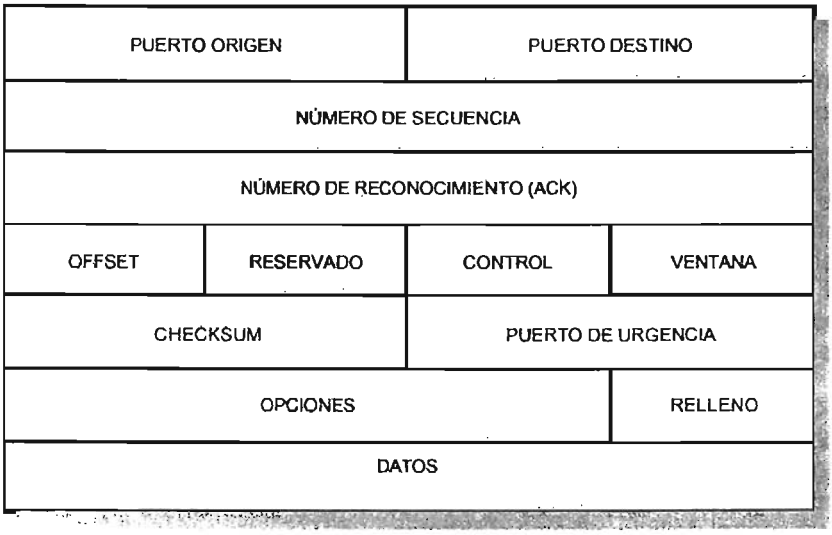


Figura 2.19 Formato de los segmentos TCP

- **Puerto Origen**: Puerto a través del cual una aplicación invoca a TCP. Su tamaño es de 16 bits.
- **Puerto Destino**: Puerto de la aplicación en destino. Su tamaño es de l6 bits.
- **Número de Secuencia**: Es el número de secuencia del primer byte de datos enviado en este segmento.
- **Número de Reconocimiento**: Es el número de secuencia del primer byte de ese segmento que se espera recibir.
- **Offset:** Contiene un entero que especifica la longitud de la cabecera de segmento en múltiplos de 32 bits. Su longitud es de 4 bits.
- **Reservados**: Estos 6 bits están reservados para usos futuros.
- **Control:** Indica el tipo de segmento. Estos seis bits indican cómo deber interpretarse algunos campos de la cabecera. Los bits están especificado. según el orden en que se enumeran, de manera que si el segundo bit tiene el valor 1, es un segmento de confirmación. La interpretación de cada bit es:

- ❖ **URG**: Segmento Urgente.
- ❖ **ACK**: Segmento de Confirmación.
- ❖ **PSH**: En TCP tanto el emisor como el receptor disponen de un buffer para almacenar los datos a enviar o a recibir. Cuando el receptor recibe un segmento con el bit de "PUSH" activado, entiende que debe envía todo lo que tiene almacenado en su buffer al proceso del cual acaba de recibir el segmento de "PUSH".
- ❖ **RST**: Segmento de Reset de Conexión
- ❖ **SYN:** Segmento que sincroniza el número de secuencia.
- ❖ **FIN**: Segmento que indica que no hay más datos para el receptor.

- ➢ **Ventana**: Indica el tamaño de la ventana.
- ➢ **Checksum**: Es un campo de 16 bits. Está formado por el complemento a 1 de la suma (en complemento **a 1)** de todas las palabras que componen el segmento **TCP**
- ➢ **Puntero Urgente**: Aunque TCP está orientado a conexión, a veces es importante enviar datos fuera de banda. Esto puede ocurrir cuando, en una conexión remota, el usuario decide enviar una secuencia de teclado que interrumpa o aborte el programa. Estas señales deben ser enviadas sin esperar a que el programa esté listo para recibir datos.

  Para acomodar el ancho de banda a las señales, TCP permite identificar estos datos como urgentes, haciendo que estos datos lleguen al destino lo antes posible. El protocolo TCP especifica que cuando unos datos son urgentes, el programa TCP del receptor debe procesarlos de inmediato y una vez procesados, volver al modo normal. Cuando el bit URG está activo, el puntero urgente especifica en la ventana la posición donde acaban los datos urgentes.

- ➢ **Opciones**: Similar al campo de opciones de IP. En ellas se especifica el máximo tamaño del segmento.

- ➢ **Relleno**: Como en IP el campo *Padding*. Son bits a cero que se utilizan para rellenar la cabecera TCP de manera que ésta alcance una longitud total que sea múltiplo de 32.

2.4.6.1.6 Encapsulamiento de la información

Mediante este mecanismo se encapsula la información de los protocolos superiores en la información de los protocolos inferiores. El encapsulamiento de los datos en TCP/IP se puede observar en la Figura 2.20

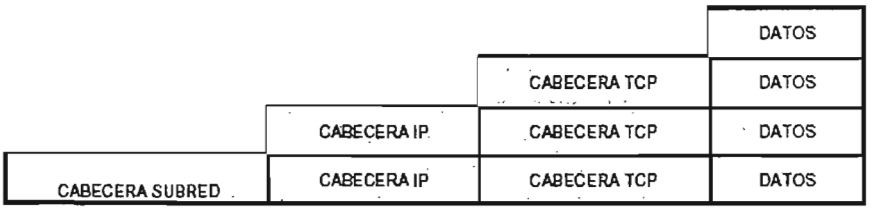


Figura 2.20

2.4.6.1.7 Establecimiento de una sesión TCP

Para el establecimiento de una sesión, TCP utiliza un mecanismo en el que se intercambian tres mensajes, tal y como muestra la Figura 2.21

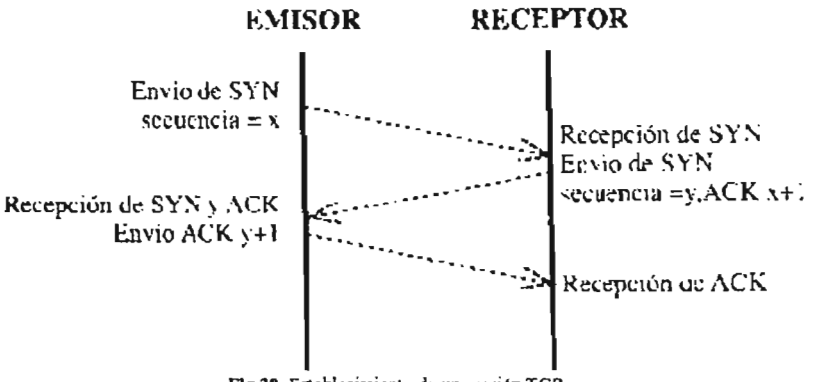


Fig 29. Establecimiento de una sesión TCP

Figura 2.21 Establecimiento de una sesión TCP

El primer segmento se identifica porque lleva activo el bit SYN en el campo de control. El segundo mensaje lleva activo tanto el bit SYN como el bit ACK. El último mensaje se usa para informar al destino que la conexión se ha establecido.

Normalmente, el proceso TCP en una máquina espera la recepción de un mensaje de este tipo, y el proceso de la otra lo inicia. Sin embargo, este mecanismo está diseñado para que ambas máquinas inicien la conexión simultáneamente. Una vez que la conexión se ha establecido, los datos pueden circular en ambas direcciones simultáneamente. no existiendo, por tanto, un maestro ni un esclavo.

El procedimiento de establecimiento de la conexión se desarrolla en los 3 pasos descritos; garantiza que los dos extremos de la transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iniciales de secuencia. Cada extremo debe elegir un número inicial de forma aleatoria. La razón es la siguiente: el protocolo TCP utiliza los servicios de IP, que no es fiable, por ello debe emplear procedimientos de temporización y retransmisión de los segmentos perdidos.

Pueden surgir problemas si los segmentos originales y retransmitidos se reciben cuando se está estableciendo la conexión, o bien cuando los segmentos retransmitidos se reciben una vez terminada la conexión. El procedimiento de establecimiento de la conexión en 3 pasos y con números de iniciación aleatorios resuelve estos problemas, pues permite distinguir los segmentos correspondientes a cada conexión.

2.4.6.1.8 Cierre de una sesión TCP.

Dos programas que empleen el protocolo TCP pueden finalizar su comunicación mediante la operación close (cerrar). Internamente, TCP emplea un mecanismo similar al de establecimiento de una sesión TCP para finalizar la conexión. Cuando un programa de aplicación comunica a TCP que no tiene más datos que transmitir, TCP finaliza la conexión en una dirección. Para cerrar esta semiconexión, el emisor TCP transmite los datos restantes y espera a que el receptor tenga conocimiento de que haya recibido estos datos, y entonces envía un segmento con el bit FIN activo. El receptor TCP recibe el segmento con el bit FIN e informa al programa de aplicación de que no hay más datos disponibles.

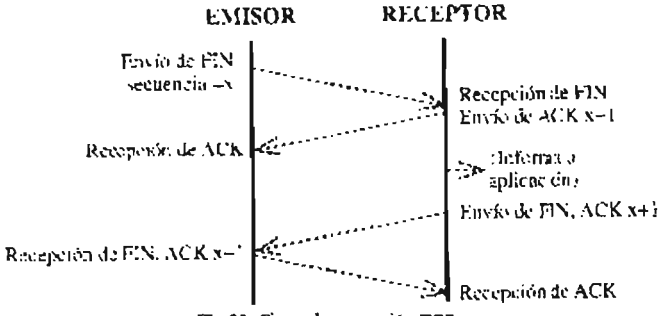


Fig 30. Cierre de una sesión TCP

Figura 2.22 Cierre de una sesión TCP

Una vez que la comunicación ha sido cerrada en un sentido, TCP no vuelve a enviar datos en este sentido. Mientras tanto, los datos pueden circular en el sentido contrario hasta que el emisor cierre la conexión. Este mecanismo puede observarse en la Figura 2.22

El procedimiento de cierre es algo más complejo que el de establecimiento de la conexión. En el cierre, una vez que el receptor recibe el segmento FIN, en lugar de generar un segmento FIN inmediatamente, envía un ACK e informa a su aplicación de la solicitud de cierre. El objeto de este ACK es tener en cuenta el posible retardo en la respuesta de la aplicación a la llegada del ACK el emisor conoce que el receptor ha recibido el segmento FIN (el enviado por el emisor) y espera hasta recibir el siguiente FIN que envía el receptor, que indica que la aplicación asociada a éste ha aceptado el cierre: el emisor responde con un ACK, con lo que la conexión se cierra finalmente.

2.4.6.2. El Protocolo UDP

El protocolo UDP es un protocolo del nivel de transporte que se basa en el intercambio de datagramas, UDP permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión (ofrece un servicio no orientado a conexión), para lo que el propio datagrama incorpora la suficiente información de direccionamiento. Esto simplifica notablemente el protocolo, pero, a cambio, no se confirman los datagramas recibidos ni se garantiza su orden, debiendo ser la aplicación la que se encargue de su control.

El protocolo UDP maneja también lo conceptos de puertos y *sockets,* ya que este protocolo es utilizado simultáneamente por varias aplicaciones (al igual que TCP). UDP básicamente proporciona acceso a los servicios del nivel IP, incorporando multipíexación/demuítiplexación. No proporciona control de flujo ni fiabilidad en las transmisiones o recuperación de algunos tipos de errores. Sirve de multiplexor/demultiplexor para el envío y la recepción de datagramas IP a través de los puertos.

2.4.6.2.1. Formato De los datagramas UDP

El formato de los datagramas UDP puede observarse en la Figura 2.23, donde:
Puerto Origen: Puerto del proceso emisor u origen (a este puerto deben dirigirse las respuestas requeridas).
Puerto Destino: Especifica el puerto del proceso destino (en el *host* destino).
Longitud: Es la longitud en bytes del datagrama UDP (incluida la cabecera).

Checksum: Es el complemento a 1 de la suma (en complemento a 1) de todos los bits que forman el datagrama UDP, más unos bits adicionales constituidos a partir de la cabecera IP.

PUERTO ORIGEN	PUERTO DESTINO
LONGITUD	CHECKSUM
DATOS	

Figura 2.23 Formato de los datagramas UDP

2.4.6.2.2 Multiplexación, Demultiplexación y Puertos

El software de UDP acepta datagramas UDP de múltiples programas de aplicación y los pasa al nivel IP para su transmisión, a la vez que acepta datagramas de IP y se los pasa a los correspondientes programas de aplicación. Conceptualmente, toda la multipíexación y demultiplexación entre el software de UDP y los programas de aplicación se realiza mediante puertos. En la práctica cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto de protocolo y un número de puerto antes de que pueda enviar datagramas UDP. Una vez que el puerto ha sido asignado, cualquier datagrama que envíe la aplicación pondrá ese número en el campo de Número de Puerto UDP.

Mientras se procesa la entrada, UDP acepta datagramas del software IP y los demultiplexa dependiendo del puerto destino UDP. En la Figura 2.24 se puede observar la demultiplexación (o multipíexación en caso de emisión) de datagramas por parte de UDP

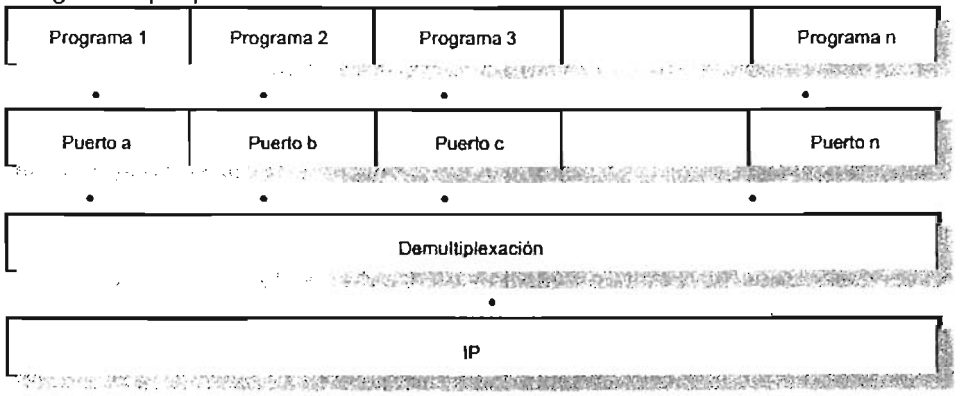


Figura 2.24 Demultiplexación de datagramas UDP

2.4.7. Nivel de aplicación

En este apartado se describen algunos de los servicios de aplicación más utilizados en la arquitectura TCP/IP. Las relaciones con la torre de protocolos TCP/IP se representa en la Figura 2.24 . Es interesante indicar que todas las aplicaciones TCP/IP se basan en el modelo cliente/servidor.

- ✓ Llamadas a procedimientos remotos (RPC)
- ✓ Conexión remota. TELNET

- ✓ Correo electrónico. SMTP
- ✓ Acceso a ficheros remotos. FTP, TFTP, NFS

2.4.7.1. Llamadas a procedimientos remotos (RPC)

Un RPC es una llamada a un procedimiento que se ejecuta en un sistema diferente del que realiza la llamada, ésta es la razón por la que el procedimiento se denomina "remoto".

En una RPC el código de programa que realiza la llamada y el procedimiento llamado se comunican a través de una "interfaz RPC" que consiste en un conjunto de operaciones y datos que sirven de "contrato" para un conjunto de procedimientos remotos.

RPC sigue el esquema cliente/servidor. El proceso que llama (cliente), envía un mensaje al proceso servidor y espera una respuesta. Por otra parte el proceso servidor se encuentra sumido en un estado de espera de peticiones y al recibir un mensaje de un cliente estudia los parámetros del procedimiento llamado obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta (véase Figura 2.25).

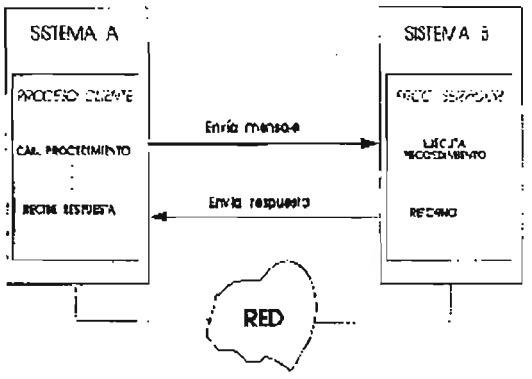


Fig.34. Procedimiento RPC [illegible]

Figura 2.25 Procedimientos RPC

Existen dos tipos de servidores:

El **servidor iterativo:** es un servidor que inicialmente se encuentra a la espera de peticiones. Cuando le llega un mensaje de petición procedente de un cliente abandona el estado de espera proporciona el servicio que le ha sido requerido

(devuelve los resultados) y vuelve al estado de espera de nuevas peticiones (véase Figura 2.26).

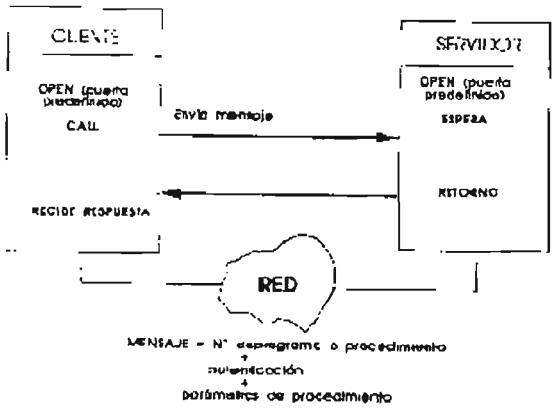


Figura 2.26

El **servidor concurrente:** es un servidor que, al igual que el anterior, inicialmente se encuentra en un estado de espera de peticiones. Si le llega un mensaje de petición, contesta al mensaje enviando al cliente un número de puerto (a través del cual el cliente recibirá su servicio) e inmediatamente arranca un proceso paralelo que presta el servicio requerido al cliente. Tras arrancar el proceso paralelo, el servidor vuelve al estado de espera en el que se encontraba inicialmente (véase Figurà 2.27).

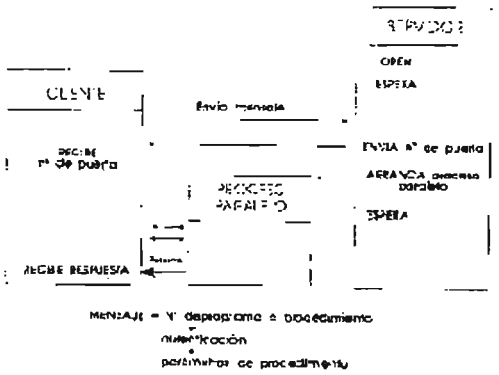


Fig.36 Servidor concurrente

Figura 2.27

2.4.7.2. Conexión remota TELNET

Principios de operación.

Este tipo de aplicación permite que un usuario en una terminal pueda acceder a recursos y aplicaciones de varios ordenadores, a través de redes, apareciendo para el usuario del terminal como si estuviese conectado localmente al ordenador remoto. Para poder conectar terminales heterogéneas a ordenadores también heterogéneos es necesario definir lo que se denomina un protocolo de terminal virtual, VTP. Un VTP es un protocolo que realiza básicamente las siguientes funciones:

- Establecimiento y mantenimiento de conexiones
- Control del diálogo para negociar las acciones permitidas durante la conexión
- Creación y mantenimiento de una estructura que representa el estado del terminal
- Traslación de las características del terminal real a la representación normalizada

En definitiva, el objetivo principal de una terminal virtual consiste en transformar las características de una terminal real en un terminal normalizado. Es prácticamente imposible definir una única terminal virtual que pueda realizar todas las funciones de las terminales existentes, por lo que normalmente se definen las funciones básicas, como modo línea para terminales sin inteligencia local, tipo teclado-pantalla/impresora, modo página en la que los caracteres pueden direccionarse a nivel de página mediante un cursor o modo gráficos.

En general, un VTP tiene las siguientes fases de operación:

- Establecimiento y liberación de la conexión
- Negociación
- Control
- Transferencia de datosLa negociación se utiliza para determinar el conjunto de características del diálogo entre los extremos de la conexión. El control realiza el intercambio de información de control y mandatos.

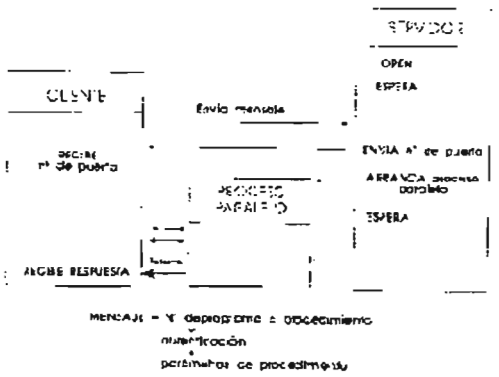


Fig.36 Servidor concurrente

Figura 2.28 Servidor concurrente

En la Figura 2.28 se representa la arquitectura de niveles de la terminal virtual.

Entre las VTP más conocidas está TELNET que fue desarrollada sobre los protocolos TCP/IP.
También se están realizando esfuerzos dentro de ISO para definir una VTP más generalizada si bien parece que uno de los conjuntos básicos que se va a adoptar es precisamente TELNET.

TELNET se fundamenta en tres principios:

- El concepto de terminal virtual, NVT Network Virtual Terminal
- Simetría entre terminales y procesos
- Opciones negociadas

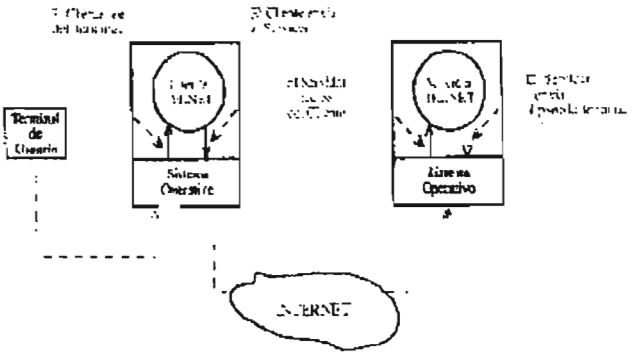


Figura 2.29

En la Figura 2.29 se representa la operación cliente/servidor de TELNET.

En la práctica, el servidor es más complejo de lo que se muestra en la figura 38 debido a que maneja múltiples conexiones concurrentes. Normalmente, un proceso servidor maestro espera nuevas conexiones y genera procesos esclavos o hijos que manejen cada una de ellas. El servidor de TELNET que se muestra en la figura representa al proceso esclavo que maneja una conexión en particular. La figura no muestra que el servidor maestro esté en un estado de escucha de nuevas conexiones.

Cuando un usuario invoca la aplicación TELNET, un proceso de usuario se convierte en la aplicación cliente. Este cliente establece una conexión TCP con el servidor, a través de la cual se comunicarán ambas entidades: una vez establecida la conexión, el cliente va aceptando los datos que teclea el usuario y se los envía al servidor.

El procedimiento de operación es similar al siguiente:

telnet nombre_de_host
Username: **xxxxxx**
Password: **yyyyyy**

Se representan en negrilla los datos que debe teclear el operador del terminal. El puerto estándar del servidor TELNET es el puerto 23.

Se pueden utilizar submandatos. Para ello se introduce únicamente el mandato telnet:

telnet>

Los principales submandatos son:

open nombre_de_host: Solicita una conexión
close: Cierra la conexión
quit: Cierra la conexión y termina el proceso local
status: Solicita el estado de la conexión
help: Solicita ayuda en línea

Para permitir que TELNET interopere con distintos sistemas han debido tenerse en consideración la heterogeneidad de los mismos, así como de sus sistemas operativos. Por ejemplo, algunos sistemas requieren que las líneas de texto finalicen con el carácter 'Retorno de Carro" *(Carriage Return* - CR): otros, sin embargo, requieren el carácter *Line feed (LF),* mientras que otros requieren ambos.

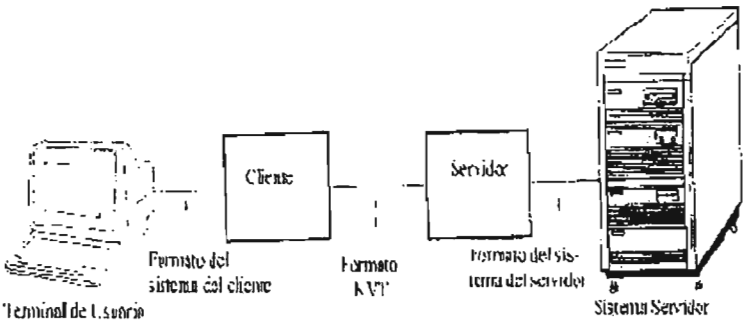


Fig.39.Mecanismo de terminal virtual utilizado por TELNET

Figura 2.30

Para permitir esa heterogeneidad de los sistemas, TELNET define cómo han de ser los datos y las secuencias de mandatos que han de circular por la red, definición conocida como *terminal Virtual de Red (NVT)*. La Figura 2.30 muestra el mecanismo con el cual se consigue este propósito. La comunicación puede ocurrir entre dos terminales, dos procesos o bien entre un terminal y un proceso. En la Figura 2.31 se representan los caracteres de control que forman parte del teclado virtual de NVT

Código de control ASCII	Valor decimal	Significado
NULL	0	No hay operación
BELL	7	Sonido audible
BS	8	Ir un carácter a la izquierda
HT	9	Ir a la derecha al siguiente tabulador horizontal
LF	10	Ir abajo a la siguiente línea
VT	11	Ir abajo al siguiente tabulador vertical
FF	12	Ir al principio de la siguiente página
CR	13	Ir al margen izquierdo de la línea actual
Otros		No hay operación (no tiene efecto de salida)

Figura 2.31 Caracteres de control del teclado NVT

Aparte de esta interpretación de los caracteres de control NVT define un delimitador de línea estándar que consta de la secuencia de caracteres CR-LF. Cuando un usuario pulsa en su terminal la tecla correspondiente a fin de línea por ejemplo ENTER), el cliente de TELNET debe transmitir CR-LF y el servidor

de TELNET lo transformará en la secuencia de caracteres apropiada para la máquina remota.

Mandatos de Control

El NVT de TELNET provee funciones de control para pasar del cliente al servidor. Por ejemplo, NVT define una tecla conceptual que posibilita la interrupción de un programa. La lista de las funciones de control que proporciona NVT se muestra en la Figura 2.32

Señal	Significado
IP	Interrupción del proceso
AO	Interrupción salida (Descartar Buffer de salida)
AYT	Verificar si el servidor responde
EC	Borrar carácter anterior
EL	Borrar linea
SYNCH	Sincroniza
BRK	Interrupción

Figura 2.32 Funciones del control que proporciona el NVT

En la práctica la mayoría de terminales no tienen definidas teclas extras para realizar determinados mandatos. El diseño de NVT separa estos mandatos del conjunto de los caracteres ASCII por dos razones:

1) La definición de funciones de manera individual le otorga gran flexibilidad. De este modo puede transferir cualquier secuencia de caracteres entre el cliente y el servidor.
2) Mediante la separación de las señales de los datos, NVT permite que el cliente defina señales de manera no ambigua.

Para transferir funciones de control mediante conexiones TCP, TELNET las encapsula en secuencias de escape, que son octetos reservados. En TELNET existe un octeto reservado. conocido por las siglas *IAC* (Interpretar Como Mandato - *Interpret As Command),* como comienzo de una secuencia de escape. Las secuencias empleadas son las que muestra la Figura 2.33

Mandato	Valor decimal	Significado
IAC	255	Interpreta el siguiente octeto como un mandato (si se desea transmitir el dato 255 se ha de enviar IAC-IAC)
DON'T	254	Negación de petición de una opción
DO	253	Conformidad de una opción específica
WON'T	252	Negación de una opción específica
WILL	251	Conformidad de una opción específica
SB	250	Comienzo de subnegociación
GA	249	Señal de continuar
EL	248	Señal de borrar línea
EC	247	Señal de borrar carácter
AYT	246	Señal de testeo del servidor
AO	245	Señal de cancelación de salida
IP	244	Señal de interrumpir proceso
BRK	243	Señal de interrumpir
DMARK	242	Secuencia para SYNCH
NOP	241	No hay operación
SE	240	Fin de opción de subnegociación
EOR	239	Fin de registro

Figura 2.33 Mandatos TELNET que han de ir procedidos de IAC

Opciones de TELNET

En TELNET las opciones son negociables permitiendo que el cliente y servidor reconfiguren sus conexiones. Por ejemplo los datos se pueden pasar como palabras de 7 bits y por el contrario emplear 8 bits para la información de control. Sin embargo TELNET provee una opción que permite que el cliente y servidor intercambien datos de 8 bits. Para ello deben negociarlo previamente.

Las posibilidades de opciones son muchas. Por ejemplo el protocolo inicial era semidúplex por los que la transmisión en el sentido contrario debía ir precedida del mandato "Continuar" (GA). Otra de las opciones es para enlace dúplex. La Figura 2.34 muestra las opciones más comunes.

Nombre	Código	RFC	Significado
Trans. binaria	0	856	Cambiar la Transmisión a binario de 8 bits
Echo	1	857	Permitir a una de las Partes de la Conexión el eco de los datos
Suprimir CA	3	858	Suprimir la Señal CA Después de Datos
Estado	5	859	Pedir el Estado de una Opción de Telnet
Marca de tiempo	6	860	Petición de que se Inserte una Marca de Sincronización
Tipo de terminal	24	884	Intercambiar Información Sobre los modelos de terminal que están siendo empleados
Modo de línea	34	1.116	Emplear Modo de Edición Local y envío de datos por líneas y no por caracteres
Línea de Fin de registro	25	885	Terminar Envío de Datos con el Código EOR
Modo 3270	29	1.041	Emulación del terminal 3270

Figura 2.34 Opciones mas usadas por TELNET

En TELNET la conexión comienza con una fase de negociación de opciones. En esta fase se utilizan cuatro mandatos: W'ILL, WONT, DO, DONT, que están incluidos en la lista de la Figura 2.33

WILL X se envía por una de las entidades para mostrar su deseo de comenzar a utilizar la opción X. También se aplica para confirmar la utilización de la opción X, DO X y DONT X se utilizan como reconocimiento positivo y negativo, respectivamente. DO X se envía para indicar a la entidad remota que comience a utilizar la opción X o bien se confirma su utilización, WILL X y WONT X se utilizan como respuesta positiva o negativa.

Un ejemplo de negociación de opciones es el siguiente:

IAC DO Tipo_de_terminal *** ¿Desea negociar el tipo de terminal?
IAC WILL Tipo_de_terminal *** Sí, Negociaré el tipo de terminal

A continuación se negociarán las características del terminal, por ejemplo, VTI00 ó 3270. En la Figura 2.35 se representa la estructura de un mandato.

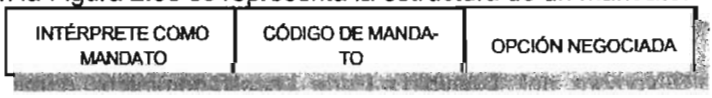


Figura 2.35 Estructura de un mandato

2.4.7.3. Correo electrónico (SMTP)

El correo electrónico es probablemente el servicio más popular entre los usuarios de red debido principalmente a que proporciona una transferencia de información de manera rápida y eficiente. Un usuario puede enviar correo a otro o mantener una conversación con un grupo de personas.

El correo no es interactivo. Cuando un usuario tiene un mensaje que enviar a otro usuario que no está conectado el sistema del correo debe tomar ese mensaje y guardarlo en una cola. Existen por tanto, dos partes conceptualmente distintas en un sistema de correo: por un lado, un proceso *front-end* que acepta correo de un usuario y lo coloca en un *área de spool,* mientras que, por otro, existe un proceso que extrae esos mensajes del área de *spool* y los envía al destino.

De esta forma un usuario puede comunicarse con otros aunque éstos no estén activos. El área en donde se depositan los mensajes recibidos hasta que el destinatario los recibe se denomina buzón.

Las funciones básicas de un correo electrónico son las siguientes:

- Creación: El usuario crea y edita un mensaje, generalmente utilizando medios locales de
- edición.
- Emisión: Se envía el mensaje a los destinatarios y se almacena en los correspondientes
- buzones
- Recepción: El destinatario accede al mensaje almacenado para efectuar su lectura
- Almacenamiento: tanto el emisor como el destinatario pueden almacenar el mensaje en un fichero

Direcciones de Correo Electrónico

Una dirección de correo identifica al sistema de correo a quien va dirigido el mensaje. A pesar de que algunos sistemas de correo poseen direcciones complicadas, las direcciones empleadas por Internet son bastante simples. Estas tienen el formato definido en el documento RFC-822.:

Parte_Local@Nombre_del_ Dominio = Parte_Local@dominio(n),dominio(n-1).... Dominiol

donde la parte local es el nombre del buzón situado en el nombre del dominio.

Por ejemplo.
jgarcia@ull.es
shernanz@pg.pres8
dpadral@tid.esp

2.4.7.3.1 El protocolo SMTP

TCP/IP define un estándar para el intercambio de correo entre dos máquinas denominado SMTP *(Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo)*. Este estándar especifica el formato exacto de los mensajes que un cliente debe enviar en una máquina al servidor en la otra. El protocolo SMTP especifica qué mensajes deben intercambiar las máquinas, pero no especifica cómo debe almacenarse el correo o con qué frecuencia se debe intentar enviar mensajes.

La comunicación entre el cliente y el servidor se lleva a cabo mediante mensajes legibles. Aunque SMTP define un formato para los mandatos, una persona puede leer fácilmente las interacciones entre cliente y servidor. Esta interacción se representa en la Figura 2.36 . Inicialmente el cliente establece una conexión al servidor y espera a que éste le devuelva un mensaje del tipo *220 READY FOR MAIL*. Si el servidor está sobrecargado debe retardar el envío del mensaje 220. Una vez que el cliente recibe este mensaje, envía un mandato *HELO*. El fin de línea marca el fin del mandato. El servidor responde identificándose. Una vez que la comunicación ha sido establecida, el emisor puede transmitir uno o más mensajes de correo, finalizar la conexión o interrogar al servidor para intercambiar papeles de emisor y receptor y permitir el intercambio de mensajes en sentido opuesto. El receptor debe enviar la conformidad con la recepción de cada mensaje.

CLIENTE	SERVIDOR
Establece la conexión ---->	
	<---- 220 READY FOR MAIL
HELLO---->	
	<-----250 OK
MAIL FROM --->	
	<-----250 OK
DATOS ----->	
	<----- START MAIL INPUT
.	
.	
.	
<CRLF><CRLF>	
	<-----250 OK
QUIT ---->	
	221 CIERRE DE CONEXIÓN

Figura 2.36

Las transacciones de correo comienzan con un mandato MAIL que envía el cliente junto con un identificador en el campo FROM que contiene la dirección a donde deben de ser enviados los mensajes de error. Se preparan estructuras de datos para recibir nuevos mensajes de correo, respondiendo el servidor al mensaje MAIL con el mensaje *250 OK*. Esta respuesta significa que todo ha ido bien.

Tras un mandato MAIL llevado a cabo con éxito, el emisor envía una serie de mandatos RCPT que identifican los recipientes del mensaje de correo. El receptor recibe cada uno de ellos y contesta con un mensaje *250 OK* si está bien o con un mensaje de error *550 No such user here*.

Tras esto se envían los mandatos *DATA*. El receptor contesta con mensajes *354 Start mail input* y especifica una secuencia de caracteres usados para finalizar los mensajes de correo. La secuencia de finalización consiste en 5 caracteres: retorno de carro, *line feed,* punto, retorno de carro y *line feed.* Hay que señalar que los sistemas de correo normalmente ocultan al usuario las interacciones descritas, proporcionando interfaces mucho más amigables.

2.4.7.4. Acceso a ficheros

El acceso a ficheros compartidos se puede ver desde dos perspectivas: acceso ***en línea,*** en tiempo real, o mediante ***copia completa.*** Compartir mediante acceso en línea significa que múltiples programas acceden a un fichero concurrentemente, por lo que los cambios que se efectúan en el fichero se llevan a cabo al momento y están disponibles para todos los procesos que acceden al fichero. El acceso por copia completa significa que cuando un programa quiere acceder a un fichero realiza una copia del mismo en local. Este último mecanismo es usado frecuentemente para datos de sólo lectura, pero si el fichero es modificado, el programa realiza el cambio en la copia local y transfiere la modificada al sitio original.

2.4.7.4.1. Acceso mediante transferencia de ficheros (FTP-TFTP)

El esquema de transferencia requiere un proceso de dos pasos: el primero consiste en obtener una copia en local del fichero. La mayoría de los mecanismos de transferencia de ficheros operan fuera del sistema de ficheros local. El usuario invoca a un programa cliente para que transfiera el fichero, debiendo especificar el ordenador remoto dónde está el fichero, llevándose a cabo una autorización de dicha operación. El cliente contacta con el servidor remoto y pide una copia del fichero, Una vez que la transferencia ha sido llevada a cabo, el usuario finaliza el cliente y el programa accede a ese fichero en su sistema local para leer y actualizar.

Este mecanismo, como ocurre con el de compartición de ficheros en línea, puede resultar bastante complejo. El cliente y el servidor deben estar de acuerdo en autorizaciones, propiedad de ficheros, protecciones y formato de datos. Este último aspecto es muy importante. Considérense dos máquinas A y B, que emplean distintos formatos para representación de números en coma flotante y para ficheros de texto. Para el primer caso es imposible llevar a cabo esta conversión del formato de una máquina al de la otra sin perder precisión. Supóngase que la máquina A almacena textos en líneas de longitud
variable y el sistema B lo realiza mediante líneas de longitud fija. La transferencia de ficheros de A a B se puede llevar a cabo rellenando las líneas a esa longitud fija, haciendo que la copia final difiera de la original.

2.4.7.4.1.1. El protocolo FTP

La transferencia de ficheros con el protocolo *FTP (File Transfer Protocol)* es **una** de las más utilizadas, FTP proporciona facilidades para las funciones de transferencia, como son:

- **Acceso Interactivo**: Si bien FTP está diseñado para ser usado por programas, la mayoría de las implementaciones proporcionan al usuario una interfaz con servidores remotos para importar o exportar ficheros.
- **Especificaciones de Formato**: FTP permite al cliente especificar el tipo y el formato de los datos. Por ejemplo, puede especificar que los datos sean ASCII o binarios.
- **Control de Autenticación**: FTP exige al cliente que se identifique mediante su nombre de usuario su contraseña. El servidor puede negarle el acceso en caso de que ese usuario no estéautorizado.

Al igual que otros servidores, la mayoría de las implementaciones de FTP permiten el acceso concurrente de varios clientes. Los clientes emplean TCP para conectarse al servidor. En general, en este tipo de servidores, el proceso maestro del servidor genera un esclavo para atender a cada uno de los clientes. En FTP, el proceso maestro acepta y lleva a cabo las peticiones de conexión del cliente, pero emplea otro proceso para manejar la transferencia de datos. Este modelo puede observarse en la Figura 2.37

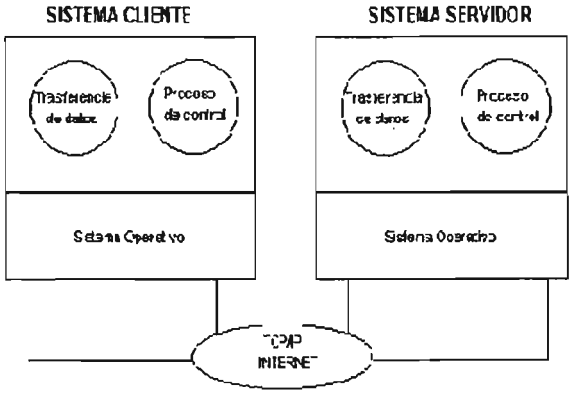


Fig.47. Esquema del funcionamiento de FTP

Figura 2.37 Esquema de funcionamiento de FTP

Como muestra la figura, el proceso cliente se conecta al servidor mediante una conexión TCP, mientras que la transferencia de datos emplea sus propias conexiones TCP. En general, el proceso de control y la conexión de control permanecen activas mientras el usuario mantenga su sesión FTP abierta. Sin embargo, FTP establece una nueva conexión de transferencia para cada fichero que se vaya a transmitir.

La conexión para transferencia de datos y los procesos de transferencia de datos se crean dinámicamente según se van necesitando, mientras que la conexión de control permanece activa mientras perdure la sesión FTP. Una vez que la conexión de control desaparece, la sesión finaliza y los procesos de ambos extremos finalizan la transferencia de datos.

Asignación de Número de Puerto TCP

Cuando un cliente se conecta al servidor, el cliente emplea un puerto aleatorio, pero el servidor se conecta en el puerto 21. Cuando el proceso de control crea una nueva conexión TCP para la transferencia de datos, no puede emplear los mismos números de puertos empleados en la conexión de control. El cliente obtiene un puerto no usado de su máquina y lo emplea para el proceso de transferencia de datos. El proceso de Transferencia de datos en la máquina servidora se lleva a cabo mediante el puerto 20 (puerto reservado a la transferencia de datos).

Visión de FTP

Los usuarios ven a FTP como un sistema interactivo. Una vez que se ha invocado, el cliente ejecuta una serie de submandatos. En la figura 48 se representa un ejemplo de transferencia de un fichero.

$ ftp

FTP user (DG/UX TCP/IP Release 5.4R2.01) ready.
ftp> **open pres8**
ftp> Connected to pres8
220 pres8 FTP server (DG/UX TCP/IP Release 5.4R3.10) ready.

Name (pres8:root): **santi**
331 Password required for santi.
Password (pres8: santi): ??????
230-User santi: working directory set to /home/santi.
230 User santi logged in. No account needed.

ftp> **type ascii**
ftp> 200 TYPE A N ok.

Using ascii type to transfer files.
Using non-Point FROM.

ftp> **help**
ftp> Command may be abbreviated. Command are:

!	debug	mdir	quote	status		
abon	dir	mget	recv	struct		
account	disconnect		mkdir	reinit	sunique	
append	exit		mls		remotehelp	type
bell	get		mode		rename	user
binary	glob		mput	restart	verbose	
bye	hash	open	rmdir	?		
cd	help	prompt	runique			
cdup	lcd	put	send			
close	ls	pwd	sendport			
delete	mdelete		quit	site		

ftp> **lcd /home/sistema**
ftp> Local directory now /home/sistema

ftp> **cd /home/santi/compiladores/sql**
ftp> 250 CWD command okay.

ftp> **ls *.c**
ftp> 200 PORT command okay.
140 Opening data connection for /bin/ls (100.0.2.6,1074) (0
bytes).
cuarteto.c

errores.c
libreria.c

operac.c
sql.c
tablas.c

226 Transfer complete.
62 bytes received in 0.010 seconds 16.1 Kbytes/s)

ftp> **ls *.y**
ftp> 200 PORT command okay.
140 Opening data connection for/bin/ls (100.0.2.6,1075) (0 bytes).
parser.y

226 Transfer complete.
10 bytes received in 0.020 seconds (0.49 Kbytes/s)

ftp> **ls *.l**
ftp> 200 PQRT command okay.
140 Opening data connection for /bin/ls (100.0.2.6,1076) (0 bytes).
scanner.l

226 Transfer complete.
11 bytes received in 0.010 seconds (1.1 Kbytes/s)

ftp> **mget *.C**
mget cuarteto.c? y
200 PORT command okay.
140 Opening data connection for cuarteto.c (100.0.2.6,1078) (3257 bytes).

226 Transfer complete.
3398 bytes received in 0.060 seconds (55 Kbytes/s>
mget errores.c? **y**
200 PORT command okay.
140 Opening data connection for errores.c (100.0.2.6,1079) (9204 bytes).

226 Transfer complete.
9472 bytes received in 0.110 seconds (84 Kbytes/s)

Fig 48. Ejemplo de FTP Visión del usuario

En el ejemplo se han marcado en negrita los mandatos que debe dar el usuario. En primer lugar invoca a FTP. Posteriormente se conecta a un ordenador remoto llamado "pres8" con el nombre de usuario "santi" e introduciendo posteriormente la palabra de paso. Se pasa a modo de transferencia de datos "ascii". Se pide una ayuda de los mandatos de FTP. Posteriormente se realiza una serie de peticiones para confirmar la existencia de distintos ficheros y se realiza la transferencia de ficheros de extensión "*.c" del directorio remoto "/home/santi/compiladores/sql" al directorio local "/home/sistema". Como puede apreciarse existen mandatos para envío y recepción de ficheros, para el manejo de directorios y para el establecimiento de parámetros y modos de transferencia.

Para las conexiones vía Internet a otros *hosts* de la red para la transferencia de ficheros, existen dos nombres de usuarios que suelen estar definidos en las máquinas con acceso a Internet y que no necesitan palabra de paso. Estos usuarios son **"anonymous"** y **"ftp"**.

Por último, cabe señalar que los mensajes de control y de errores se llevan a cabo mediante mensajes de 3 dígitos seguidos de texto, de manera que son perfectamente legibles.

2.4.7.4.1.2. El Protocolo TFTP

A pesar de que FTP es el protocolo más usado para la transferencia de ficheros, también se emplea otro protocolo llamado **TFTP,** ya que muchas aplicaciones no necesitan de todas las funcionalidades que ofrece FTP: por ejemplo, FTP obliga a que el cliente y el servidor empleen múltiples conexiones concurrentes.

TFTP fue definido para aplicaciones que no necesitan tanta interacción entre cliente y servidor. Está restringido a operaciones de transferencia de ficheros en los que no es necesaria una autenticación. Por estas razones los protocolos TFTP son más sencillos.

La simplicidad es particularmente importante para algunas aplicaciones. Por ejemplo, los diseñadores de estaciones de trabajo sin disco pueden incluir el software TFTP en memorias de sólo lectura (ROM). El programa en ROM se llama **bootstrap.** La ventaja de TFTP es que permite el arranque en remoto. Así es posible que un ordenador arranque desde un servidor.

TFTP emplea el puerto 69 que previamente debe estar asignado. Emplea el protocolo UDP en vez de **TCP.** La corrección de errores se realiza a nivel TFTP, es decir, utiliza un mecanismo de parada y espera para controlar el flujo de

información. El emisor envía los ficheros por bloques de tamaño fijo (512 bytes)y espera confirmación por parte del receptor. El receptor tiene que enviar la conformidad de la recepción de cada bloque de datos.

Las reglas para TFTP son muy simples. En el envío del primer paquete se establece una interacción entre el cliente y el servidor. Se empieza una numeración de bloques comenzando por el 1. Cada paquete de datos contiene una cabecera que especifica el bloque que contiene, y por cada confirmación contiene el número de bloque que confirma su recepción. Un bloque de menos de 512 bytes implica que es el final del fichero.

La Figura 2.38 muestra el formato de cinco tipos de paquetes TFTP. El paquete inicial emplea el código de operación 1 ó 2 especificando si es una lectura o una escritura. También contiene el nombre del fichero y los modos de acceso de la petición del cliente (lectura o escritura).

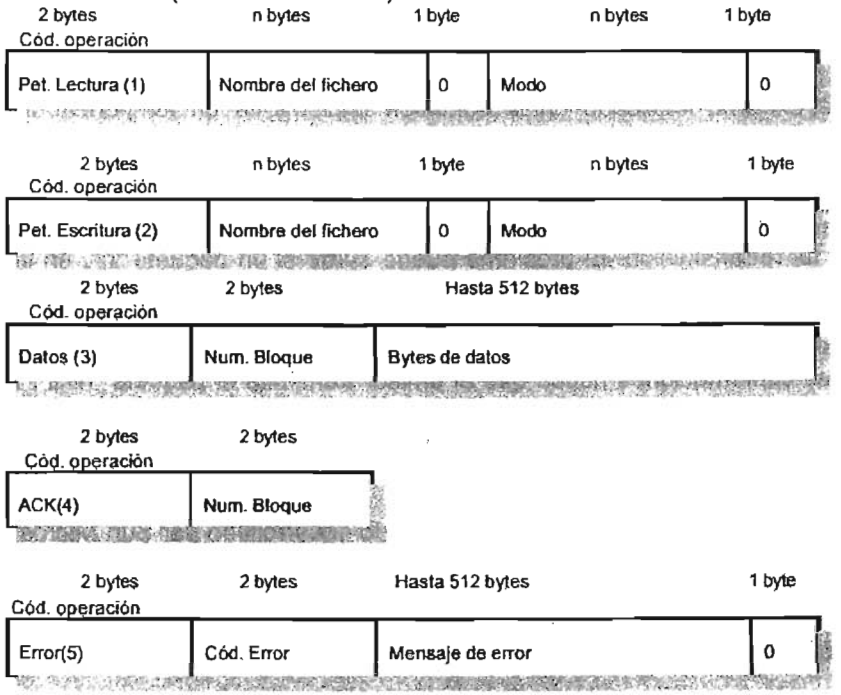


Figura 2.38 Ejemplos de mensajes TFTP

Una vez que se ha efectuado una petición de lectura o escritura, el servidor emplea la dirección IP y el protocolo UDP del cliente para siguientes operaciones. Ni los mensajes de datos ni los de confirmación de recepción (ACK) necesitan incluir el nombre del

fichero. Los mensajes perdidos pueden ser retransmitidos cuando vence un temporizador, pero la mayoría de los errores provocan la finalización de la transmisión. En la Figura 2.39 se representa el flujo de transferencia TFTP.

CLIENTE	SERVIDOR
Petición lectura ----->	
	<----- DATOS (BLOQUE 1)
ACK (BLOQUE 1) ----->	
	<----- DATOS (BLOQUE 2)
ACK (BLOQUE 2) ----->	
.	.
.	.
.	.

Figura 2.39 Transferencia TFTP

Cada extremo implicado en la conexión implementa un temporizador y una retransmisión. Si vence el temporizador del emisor, éste retransmite el último bloque de datos. Si vence el temporizador del receptor, éste retransmite la última confirmación.
A pesar de que la retransmisión simétrica garantiza robustez, puede resultar cara tal retransmisión. El problema puede surgir si un paquete "n", en lugar de perderse, simplemente se demora. El emisor retransmite el paquete de datos mientras el receptor emite la confirmación. Ambas confirmaciones llegan y se transmite el paquete "n+1". El receptor confirma ambas copias del paquete "n+l" y tales confirmaciones hacen que el emisor transmita el paquete "n+2". El ciclo continúa y provoca que cada paquete de datos sea transmitido dos veces.

2.4.7.4.2. NFS (Network File System)

El sistema de ficheros de red o NFS ha sido desarrollado por Sun Microsystems y autoriza a los usuarios el acceso "en línea" a ficheros que se encuentran en sistemas remotos, de esta forma el usuario accede a un fichero remoto como si éste fuera una fichero local. Desde la perspectiva del usuario, NFS es casi invisible.

Cuando un programa de aplicación se ejecuta, como muestra la Figura 2.40, un proceso cliente realiza una llamada al sistema operativo, bien para abrir un fichero o bien para almacenar datos en el fichero. El mecanismo que rige el acceso a los ficheros acepta la petición y automáticamente la pasa, dependiendo de si el fichero se encuentra en el disco local o en el ordenador remoto, al

sistema de ficheros local o al cliente NFS. Cuando se recibe la petición, el proceso cliente utiliza el protocolo NFS para contactar con el proceso servidor adecuado en la máquina remota y así realizar el servicio requerido. Una vez que el proceso servidor devuelve los resultados correspondientes, el cliente reenvía estos resultados al programa de aplicación, finalizando así la cooperación entre el cliente y servidor.

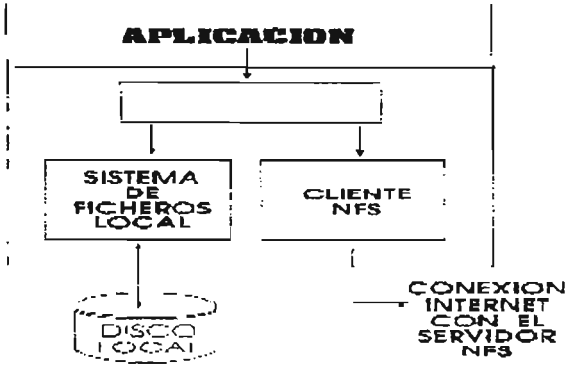


Fig. 51

Figura 2.40

Para llevar a cabo este servicio son necesarios dos protocolos:

- El **protocolo MOUNT**, que especifica el *host* remoto y el sistema de ficheros al que va a acceder.
- El **protocolo NFS**, que realiza las tareas de entrada/salida del fichero remoto.

Ambos protocolos son aplicaciones RPC (de llamada a procedimientos remotos), y utilizan el servicio de transporte UDP.

2.4.7.4.2.1. El protocolo MOUNT

Se trata de un servidor RPC que realiza cinco funciones:

- **NULL**: operación nula. Sirve para que el ordenador se autoverifique.
- **MOUNT**: monta una unidad de disco, un directorio o un conjunto de ficheros externos, en el sistema de ficheros local del *host:* de esta forma, el *host* los puede tratar como si formaran parte de uno de sus subdirectorios.
- **DUMP**: devuelve una lista de los ficheros montados en el sistema.

- **UNMOUNT**: desmonta del sistema de ficheros una lista de ficheros que se le da como parámetro.
- **EXPORT**: proporciona información sobre los sistemas de ficheros que se encuentran disponibles.

2.4.7.4.2.2. EL Protocolo NFS

Una vez que se ejecuta el mandato "MOUNT", el protocolo NFS se encarga de realizar todas las operaciones básicas de entrada/salida de ficheros. NFS da soporte a 18 procedimientos que cubren todas estas operaciones básicas. A continuación se exponen algunas de ellas:

- **LOOKUP**: Busca un fichero en el directorio actual de trabajo.
- **READ/WRITE**: son las dos primitivas básicas de acceso a un fichero para leer o escribir.
- **RENAME**: renombra un fichero.
- **REMOVE**: borra un fichero.
- **MKDIR / RMIDIR**: creación y borrado de directorios.

Una vez que se monta el directorio remoto en un *host*, el sistema operativo local al *host* debe encargarse de "reencaminar" estas primitivas de entrada/salida al *host* remoto. De esta forma el servicio proporcionado por el protocolo NFS resulta totalmente transparente al usuario (véase Figura 2.41)

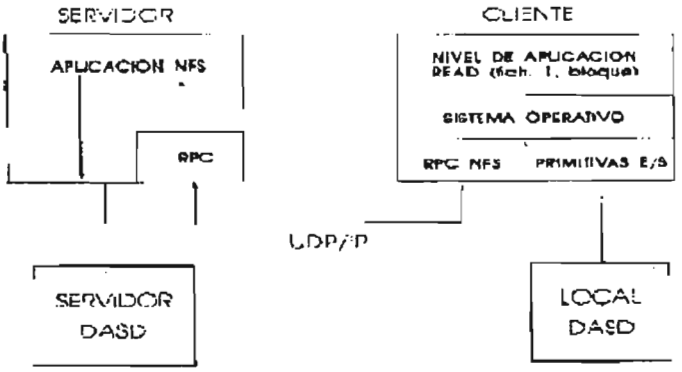


Fig.52.

Figura 2.41

2.5. Principales servicios disponibles en Internet

Los servicios más conocidos proporcionados a través de Internet son por una parte las aplicaciones estándar de TCP/IP como correo electrónico, transferencia de ficheros FTP, conexión remota Telnet etc así como nuevas aplicaciones como Foros (Usenet o News) **ARCHIE, GOPHER. WAIS. y** el más llamativo. el **World Wide Web, WWW,** la famosa tela de araña con cobertura universal.

Los foros de Internet proporcionan básicamente las mismas funciones que se encuentran en las conferencias de las BBS. En defininiva, las BBS, *Bulletin Board Systems.* son. simplificando. una forma electrónica de tablones de anuncio en el que los usuarios dinámicamente depositan sus mensajes.Cuando otro usuario ve un mensaje que le interesa crea un comentario o apunte que se enlaza con el anterior. De esta forma se pueden establecer conferencias electrónicas. tan populares entre los usuarios de Internet. Usenet. más conocido como Netnews o News, es un servicio de información con más de
3.000 grupos de interés, en donde usuarios de todo el mundo hacen y responden preguntas. opinan. anuncian o ven lo que otros hacen. Hay grupos de conversación sobre los temas más diversos. Como ordenadores, política, ciencias sociales. deportes. gastronomía. etc.

Los servidores ARCHIE construyen dinámicamente índices de ficheros con los contenidos en los servidores FTP de internet. ARCHIE nos responde a consultas sobre la localización de ficheros. Actualmente existe un servidor ARCHIE en la mayoría de los países.

Los servidores GOPHER procesan y proporcionan información relativa a los recursos Internet, como servidores FTP, servidores ARCHIE, conferencias. etc. A través de un sencillo esquema de menús, el usuario accede a servicios de distinta índole. Los servidores GOPHER vinculan la información de todo Internet de manera transparente para el usuario: bases de datos, documentos, libros, imágenes, etc.

Los servidores WAIS, Wide Area Information Services, ofrecen un sistema de búsqueda alternativa más directa que los Gopher. Funcionan mediante palabras clave, es decir, las peticiones se componen de un grupo de palabras que identifican la información buscada. El servidor busca estas palabras en sus indices y devuelve una lista de direcciones donde encontrar documentos y ficheros que satisfagan la solicitud.

Si bien el correo electrónico es todavía el servicio más utilizado, el World Wide Web se está convirtiendo en uno de los más espectaculares y con un gran

potencial de utilización en todos los sectores de la actividad. tanto científica como económica e incluso lúdica. El WWW muestra a los usuarios una serie de páginas que pueden contener textos, gráficos, sonidos e imágenes estáticas y en movimiento. Los documentos están enlazados mediante hipertexto, cuya característica principal es que los documentos contienen "enlaces", es decir, palabras que hacen referencia a otros documentos relacionados con el tema. Cuando se selecciona un vocablo realzado se puede pasar a la siguiente página del mismo documento o bien conectarse con otro punto del Web en otro lugar del mundo que tenga información relacionada. Con un programa visualizador, como Netscape o Mosaic, se puede "navegar" de un documento a otro de forma muy sencilla. Muchas importantes compañías y organizaciones, como la UIT, el ATM Forum, las Universidades, Centros científicos, etc., tienen información en Web. El mundo comercial ha tardado en utilizar los servicios de Internet, debido fundamentalmente a preocupaciones por el tema de la seguridad. Este aspecto ha mejorado notablemente. precisamente por la presión de aplicaciones como el comercio electrónico, y en la actualidad la información y los servicios de negocios han suscitado una gran expansión e interés. Muchas empresas disponen de traductores para convertir la información de sus bases de datos a HTML, el lenguaje utilizado para codificar páginas Web. Una aplicación de estos traductores es la prensa electrónica. El diario electrónico está en las páginas Web y pasa a la base de datos para su archivo una vez que es reemplazado. Sin embargo. en caso de que un usuario efectuase una consulta, automáticamente se cargaría el tema seleccionado en las páginas Web.

Para conseguir una seguridad robusta se utilizan técnicas criptográficas complementadas con otras como la llamada de "huellas digitales". La criptografía se basa en la utilización de parejas de claves: una secreta y otra pública. Con ello se consigue no sólo la protección de la información, sino también su autenticación. La técnica de las "huellas digitales" se basa en añadir unos caracteres a la información derivados del contenido de ésta. De esta forma se garantiza la integridad del contenido de la información aunque se difunda ampliamente o se bagan copias. Con esta técnica se pueden detectar tanto manipulaciones fraudulentas. como virus, como no intencionadas, como errores en las copias. en la transmisión. etc. También puede conseguirse que la información sea solamente legible para los destinatarios deseados.

Muchas empresas han desarrollado procedimientos de seguridad para operar en Internet. como IBM con cryptologos. Netscape ha diseñado un sistema de *sockets* cifrados que permiten accesos WWW seguros. CyberCash es una iniciativa prometedora. ya que ha conseguido momentáneamente el permiso del Departamento de Comercio de EE.UU. para exportar tecnología de seguridad. Existen intentos de establecer pautas generales de seguridad en Internet. como un borrador reciente que describe protocolos de autenticación y cifrado. "*A*

Certificate Management Application Programming Interface", con fecha de marzo de 1995. La empresa Terisa ha tomado el testigo para desarrollar una norma única para transacciones comerciales. Como nota curiosa. el gobierno canadiense ha puesto en marcha un proyecto para utilizar criptografía en clave pública para tarjetas personales, con el fin de proporcionar servicios de comercio electrónico básico, correo electrónico privado y otros servicios. Se prevé que este proyecto comience a operar en 1997.

Los desarrolladores de *software* están comenzando a desarrollar aplicaciones que pueden estar distribuidas en Internet a través de *WWW* o de otros frontales que se están desarrollando actualmente. **Java** (nombre coloquial con el que en EE.UU. se refieren al café), es un lenguaje de SUN basado en objetos y sistemas abiertos que facilita la creación de aplicacciones distribuidas en Internet. También es un ordenador virtual (máquina virtual Java) que eventualmente permitirá que las aplicacciones puedan ejecutarse en cualquier ordenador, con independencia de su *hardware* y sistema operativo.

Con las mejoras de seguridad, en la actualidad se piensa que el comercio electrónico puede ser una de las aplicaciones más atractivas de Internet. En definitiva, lo que empezó como una red de carácter marcadamente científico se está convirtiendo en un canal ampliamente utilizado por las organizaciones y compañías de diversos sectores de negocios e incluso por el gran público.

2.5.1. Acceso a Internet

En la Figura 2.42 se representa muy esquemáticamente cómo realizar el acceso a Internet, bien desde una empresa, bien desde un usuario individual.

En a) se muestra una empresa que dispone de acceso a Internet. Los nodos formarán parte de la red autónoma y se integran en Internet a través de un encaminador externo. La IAB le proporciona a la empresa una dirección IP, por ejemplo, tipo B. La empresa dispone de libertad par administrar las direcciones de sus nodos dentro de la dirección autónoma. En el caso de direcciones tipo B, dispondrá de 2 octetos, es decir, de una capacidad superior a 60.000 nodos IP. En caso de que la empresa disponga de varias sucursales u oficinas, éstas podrán conectarse. también mediante encaminadores, a la oficina principal, en donde se encamina la información hacia Internet. En función del tráfico, los circuitos entre las sucursales periféricas y el Centro pueden ser dedicados, por RTC, Red Telefónica Conmutada o RDSI. Red Digital de Servicios Integrados.

En b) se representa el caso en el que una empresa no dispone de acceso directo a Internet, por lo que tiene que contratar los servicios a una empresa

Proveedora de Servicios a Internet. Aquí los circuitos suelen ser por RTC o RDSI.

En c) se indica la conexión de un usuario individual que dispone de una cuenta. bien en un Centro Proveedor de Internet, CPI o bien en una Institución científica o académica que disponga de acceso a Internet.

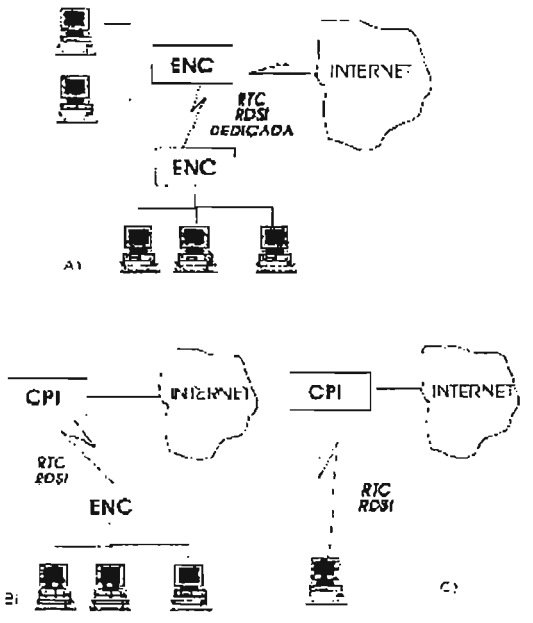


Figura 54
Figura 2.42

Los protocolos utilizados en todos los casos son TCP/IP En las conexiones punto a punto,.sean dedicadas, RTC o RDSI, se suele utilizar, a nivel de enlace, un protocolo denominado PPP, *Point to Point Protocol.* El objetivo del protocolo PPP, descrito en las RFC 1171,. 1172 y 1220 es la transmisión de datagramas multiprotocolo en líneas punto a punto. Para ello se definen 3 tipos de tramas:

- Tramas LCP, *Link Control Protocol,* para establecimiento, configuración y prueba de enlace
- Tramas *Network Control Protocol,* NCP, para establecimiento y configuración de enlace entre niveles de red
- Datagramas encapsulados en PPP

El protocolo PPP suele utilizar un procedimiento de autenticación.

En lo que respecta a nivel físico si el acceso es por RDSI, lo normal es utilizar un Canal B a 64 Kbps. En caso de utilización de RTC se recomiendan módems V.34 a 28.800 bps a ser posible con sistemas de compresión y detección de errores (MNP, V.42 y V42bis). Se pueden conseguir tasas de compresión de hasta el 80% si la información es muy repetitiva. En el caso de textos lo usual son tasas del orden del 50%.

2.6. Seguridad en entornos de red

Los mecanismos de salvaguarda de las redes de comunicaciones "no locales" entre sistemas-nodos de parecido o distinto nivel han de tener en cuenta que los canales de transporte contratados a proveedores externos pueden tener problemas de seguridad (acceso de terceras partes) fuera del dominio propio.
Estas redes suelen presentar ese y otros problemas especiales de seguridad, pues:

- Son más complejas que los equipos individuales tanto por estructura como por coordinación
- Comparten medios físicos, dispositivos de enlace y equipos accesibles
- Su perímetro es difuso, con recursos y usuarios locales que se prolongan a entornos remotos
- Los puntos de amenaza se distribuyen en múltiples lugares por los que viaja la información
- El acceso remoto permite a usuarios desconocidos acceder anónimamente a las "puertas" de los equipos, camuflando su identidad tras varios equipos y medios; los controles de autenticación y acceso han de funcionar así en un entorno mas agresivo e incierto
- La multiplicidad de rutas posibles entre dos equipos deja su elección fuera del control de los usuarios o las aplicaciones, incluso en redes de complejidad media.

Este escenario conlleva la posibilidad de amenazas de los siguientes tipos:

- **Intercepción (lectura) de datos en tránsito**, accediendo a su contenido o a su sola existencia (análisis de tráfico).
- **Modificación de datos en tránsito**, con aparición de un "tercero interpuesto" *man in the middle* que actúa de repetidor neutro durante la mayor parte del tiempo, pero que eventualmente puede retransmitir variantes alteradas de lo que recibe.
- **Acceso (lectura)** no autorizado a programas y/o datos en equipos remotos.

- **Ejecución** de programas en equipos remotos.
- **Suplantación** de la personalidad de un usuario autorizado.
- **Reproducción** ciega de transacciones registradas anteriormente.
- **Bloqueo de tráfico** (total, parcial o selectivo) realizado de forma pasiva (deja perder paquetes en tránsito) o activa (se inyecta ruido en la red).

El concepto de "cortafuegos" se ha popularizado con la difusión de Internet. Muchas organizaciones han conectado o se plantean la necesidad de conectar sus redes internas privadas (Intranets, para seguir la terminología en auge) a redes externas. La falta de dominio sobre la seguridad de éstas no debe privar a sus usuarios de dominar la seguridad de la Intranet propia y de acceder a la amplia panoplia de servicios externos, gobernados por todo tipo de protocolos, que por ejemplo proporciona Internet; sean en este caso servicios de consulta y transferencia como *ftp, tftp, telnet, http, rlogin, NFS,* sean servicios de correo como SMTP, POP3, IMAP4.

- Conviene recordar que Internet se diseñó para ofrecer gran seguridad sobre su disponibilidad global (frente a grandes catástrofes), pero no sobre la confidencialidad, autenticidad e integridad que han de garantizar muchas organizaciones privadas. Partiendo del principio de que la seguridad absoluta es una asíntota no alcanzable, las versiones actuales de TCP/IP tienen problemas técnicos de seguridad como éstos.

- **Escucha clandestina y falsificación fáciles**. La mayor parte del tráfico Internet no está cifrado. El correo, las contraseñas y las transferencias de ficheros se pueden monitorizar y capturar utilizando fácilmente el software disponible.

- **Servicios TCP/IP muy vulnerables**, particularmente los de prueba y testeo.
- **Complejidad de configuración** de los controles de acceso de seguridad a los ordenadores; si se configuran involuntaria pero incorrectamente, permiten peligrosos accesos no autorizados.

Pero la inseguridad en la conexión a las redes externas de las organizaciones se debe sobre todo a que muchas de éstas carecen de política de seguridad, entendida como un conjunto de decisiones racionales respecto a las medidas adecuadas para protegerse eficazmente. Muchas organizaciones configuran el acceso a Internet sin tener en cuenta los posibles abusos desde ésta; abren más servicios **TCP/IP** de los que requieren sus operaciones, con el consiguiente acceso de información de y sobre su red interna
a los intrusos.

2.6.1. Filtros y Cortafuegos

Los dos mecanismos básicos para afrontar las amenazas a la red interna desde las externas son:

- Filtros para control de los flujos de información (acceso, rutas y accesibilidad de terceras partes)
- Cortafuegos para proteger la información en sí (de su confidencialidad e integridad)

Los Filtros se establecen para controlar los flujos de información en los nodos siempre que sea posible.

Conviene recordar que los nodos-conectores de una red se suelen clasificar en tres niveles:

- Un conector de nivel 1 o ***repetidor*** se emplea dentro del mismo edificio para enlazar equipos cuya comunicación directa supere las características físicas del medio; no puede contener filtros, lo que tiene escaso impacto pues la zona debe estar controlada con otras políticas de seguridad.
- Un conector de nivel 2 o ***puente (bridge)*** enlaza dos subredes y reproduce el tráfico de una en otra si su origen y destino están a cada lado del puente; éste suele aprender dinámicamente qué equipos hay en ambas subredes a base de escuchar las emisiones y se suele emplear para distribuir tráfico y atajar la saturación del medio también dentro del mismo edificio, por lo que la carencia de mecanismos de filtrado también tiene escaso impacto.
- Un conector de nivel 3-4 o **enrutador *(router)*** suele enlazar dos redes unidas por canales externos al edificio atendiendo a direcciones de red y por tanto suele poder clasificar los paquetes por tipos de protocolo. Esta topología siempre tiene al menos dos puertos (más si la conexión se estructura en forma de estrella)

La política de seguridad de un ***enrutador*** exige mecanismos de filtrado específicos que han de tomar en consideración tres parámetros, las direcciones de red del remitente y del destinatario; así como el tipo de servicio (que puede inferirse del puerto al que va dirigido y/o del que procede, ya que el par "dirección-puerto" permite identificar con relativa solvencia qué servicio soporta el paquete).

En base a estos parámetros, el filtro autorizará o denegará el tránsito de un paquete desde un puerto a otro de los controlados porenrutador, con una política de seguridad del tipo "todo denegado salvo autorización expresa" que se plasmará en el control de configuración del sistema. Para implantar una política de seguridad en el enrutador se siguen estos pasos:

- Identificar al responsable de autorizar nuevas reglas y dar de baja reglas antiguas.
- Identificar al responsable de configurar los equipos.
- Asociar direcciones de red a puertos del enrutador de forma estricta para inhibir la posibilidad de que un nodo en una red enmascare a un nodo de otra *(spoofing)*
- Desarrollar una batería de pruebas, tests de regresión, que valide la implantación de la política de seguridad elegida (las pruebas se ejecutan cada vez que se altere la configuración por nueva política, inclusión o eliminación de reglas, cambio de equipo o versión de *software* o *firmware*).
- Registrar en el libro de operación del sistema las actuaciones y los resultados de las pruebas.

Un **Cortafuegos** *(firewall)* es un mecanismo de filtrado que aísla una "ciudadela segura", tratando de identificar los puntos de acceso vulnerables en el "perímetro" y de concentrar en ellos la política de seguridad en tránsito que se desee. En el caso más típico, el cortafuegos aísla una red privada del entorno constituido por la red pública externa; pero el modelo sirve también para aislar dos redes privadas entre si cuando las características de seguridad de ambas difieren notablemente.

El cortafuegos (mejor se llamaría puente levadizo) impone una política de acceso desde/hacia la red exterior, lo que parece poder relajar la política interna de seguridad de la red protegida (se deja circular dentro con más libertad). Pero el cortafuegos no influye en la política de seguridad interna y no reduce los riesgos de ataques originados internamente y dirigidos a los equipos internos.

La política de acceso que soportaría un cortafuegos es incluso la única posible en ciertos casos:

- En entornos donde la implantación de controles de acceso estrictos no es fiable en todos y cada uno de los equipos; o donde la información transita "en claro" (sin cifrar) por segmentos comunes

- En redes complejas cuya cantidad de equipos desborde la capacidad de administrar la seguridad por su responsable; éste sólo podrá imponer, mantener y monitorizar una política de seguridad con solvencia centralizando su materialización en un sólo punto y en forma de cortafuegos

El cortafuegos se materializa con un equipo único que proporciona toda la funcionalidad o con equipos separados (software, enrutador, servidor e incluso red) cuya combinación ofrece el efecto deseado. Se puede así requerir un cortafuegos multinivel, es decir una mini-red interna que se conoce como "red de nadie" o "desmilitarizada". Alrededor de este segmento de red se disponen enrutadores de acceso y/o servidores ("bastiones") que hospeden los *proxies* o programas correspondientes. Esta arquitectura dota al cortafuegos de una capacidad de concentrador, muy útil cuando hay que disponer varias puertas bajo su control. La arquitectura multinivel dota al sistema de niveles de defensa en profundidad; un ataque con éxito a uno de los componentes no conlleva la penetración inmediata; los mecanismos de alarma deben detectar la intrusión y avisar al administrador, que dispone de cierto tiempo para reaccionar antes de que se logre penetrar la siguiente barrera. Así, un cortafuegos no es un componente único, sino un concepto estratégico diseñado para proteger los recursos de la organización que pueden alcanzarse a través de Internet.

2.6.2. Tipos de cortafuegos

El cortafuegos es un dispositivo con funciones de separación, limitación y análisis, que al menos dispone de dos puertas y controla en todo caso el flujo de información entre dos de las posibles puertas. Su principal función es el control de acceso centralizado, cuya efectividad excluye poder acceder sin cruzarlo de/a las redes internas por usuarios internos/exteriores/remotos. Así, si un viajante de una empresa puede llamar mientras viaja a su PC de la oficina por medio de línea pública y modem, con ese PC conectado a la red interna protegida de la organización, un atacante puede llamar a ese PC directamente y se salta así el cortafuegos que protege la red interna de la organización. Si un usuario accede, desde su PC de la oficina utilizando el modem y la red telefónica conmutada, a su cuenta Internet abierta en un ISP (Proveedor de Servicios Internet), está abriendo una conexión no segura con Internet que se salta la protección del cortafuegos.

Un cortafuegos proporciona diversos tipos posibles de protección:

- Registra el tráfico que sale o llega a la red privada.
- Bloquea tráfico no deseado.

- Dirige el tráfico entrante a sistemas internos preparados para tal fin, más confiables.
- Oculta identificadores (topología y dispositivos de red, sistemas y usuarios internos de Internet).
- Oculta sistemas vulnerables que no pueden hacerse fácilmente seguros de Internet.
- Proporciona una autenticación más robusta que la de las aplicaciones estándar.

Pero conviene también aclarar otras protecciones que **NO** proporcionan los mitificados cortafuegos:

- No protegen contra amenazas inteligentes intencionales internas (en el dominio de la intranet)
- No protegen contra amenazas derivadas de conexiones con el exterior que no pasan por él
- No protegen contra virus ni amenazas no catalogadas

Para protegerse de estas amenazas habrá que combinar el cortafuegos con otros mecanismos de salvaguarda. Como en todo mecanismo de protección, el cortafuegos es un compromiso entre conveniencia y seguridad. Se llama transparencia a la visibilidad del cortafuegos tanto para los usuarios de dentro como los de fuera que lo atraviesan. Un cortafuegos es "transparente" para los usuarios si éstos no se dan cuenta de su presencia ni deben detenerse en él para poder acceder a la red. Los cortafuegos normalmente se configuran para ser transparentes a los usuarios de la red interna (mientras no se encuentren fuera del cortafuegos), pero no transparentes para todas las redes externas que deseen atravesar el cortafuegos. Esta política proporciona generalmente un nivel muy alto de seguridad sin cargar excesivamente a los usuarios internos.

El cortafuegos puede trabajar en tres niveles:

- *Al nivel de red,* controlando el trasiego de paquetes individuales (se denomina ***"apantallado"***).
- *Al nivel de aplicación,* controlando el acceso a servicios individuales (se denomina ***"proxy"***).
- *Al nivel de agente activo*, entrando a controlar el contenido de los accesos a los servicios (evitando virus, impidiendo el acceso a servicios de carácter no profesional, imponiendo límites al volumen de información en tránsito, etc.).

El cortafuegos debe tener características y capacidades distintas según trabaje en uno u otro nivel:

- *Volumen de tráfico* a gestionar, creciente desde el nivel de red al de aplicaciones que controlan el contenido, *"capacidad de control"* muy superior para el nivel de aplicación que para el nivel de red.
- *Registro de uso*: indiferenciado al nivel de red y con clasificación por servicios al de aplicación.
- *Identificación del usuario*: prácticamente imposible al nivel de red, pero posible al de aplicación (se llega a delegar en el cortafuegos toda la política de control de acceso, desde el exterior o el interior).

En definitiva, el cortafuegos consiste en un dispositivo informático (un enrutador o un ordenador) que separa físicamente un dominio de red de otro. Los enrutadores pueden controlar el tráfico en el nivel de red/transporte permitiéndolo o denegándolo selectivamente en base a la dirección fuente/destino y al número de puerto. Los ordenadores pueden controlar el tráfico en el nivel de aplicación. Los cortafuegos aplican un conjunto de operaciones de filtrado de paquetes del nivel red/transporte,tomando así decisiones de seguridad basadas en la información (dirección fuente y número de puerto),que proporcionan por ejemplo las cabeceras IP y TCP.

2.6.2. Tipos de cortafuegos

El cortafuegos es un dispositivo con funciones de separación, limitación y análisis, que al menos dispone de dos puertas y controla en todo caso el flujo de información entre dos de las posibles puertas. Su principal función es el control de acceso centralizado, cuya efectividad excluye poder acceder sin cruzarlo de/a las redes internas por usuarios internos/exteriores/remotos. Así, si un viajante de una empresa puede llamar mientras viaja a su PC de la oficina por medio de línea pública y modem, con ese PC conectado a la red interna protegida de la organización, un atacante puede llamar a ese PC directamente y se salta así el cortafuegos que protege la red interna de la organización. Si un usuario accede, desde su PC de la oficina utilizando el modem y la red telefónica conmutada, a su cuenta Internet abierta en un ISP (Proveedor de Servicios Internet), está abriendo una conexión no segura con Internet que se salta la protección del cortafuegos.

Un cortafuegos proporciona diversos tipos posibles de protección:

- Registra el tráfico que sale o llega a la red privada.
- Bloquea tráfico no deseado.

- Dirige el tráfico entrante a sistemas internos preparados para tal fin, más confiables.
- Oculta identificadores (topología y dispositivos de red, sistemas y usuarios internos de Internet).
- Oculta sistemas vulnerables que no pueden hacerse fácilmente seguros de Internet.
- Proporciona una autenticación más robusta que la de las aplicaciones estándar.

Pero conviene también aclarar otras protecciones que **NO** proporcionan los mitificados cortafuegos:

- No protegen contra amenazas inteligentes intencionales internas (en el dominio de la intranet)
- No protegen contra amenazas derivadas de conexiones con el exterior que no pasan por él
- No protegen contra virus ni amenazas no catalogadas

Para protegerse de estas amenazas habrá que combinar el cortafuegos con otros mecanismos de salvaguarda.

Como en todo mecanismo de protección, el cortafuegos es un compromiso entre conveniencia y seguridad. Se llama transparencia a la visibilidad del cortafuegos tanto para los usuarios de dentro como los de fuera que lo atraviesan. Un cortafuegos es "transparente" para los usuarios si éstos no se dan cuenta de su presencia ni deben detenerse en él para poder acceder a la red. Los cortafuegos normalmente se configuran para ser transparentes a los usuarios de la red interna (mientras no se encuentren fuera del cortafuegos), pero no transparentes para todas las redes externas que deseen atravesar el cortafuegos. Esta política proporciona generalmente un nivel muy alto de seguridad sin cargar excesivamente a los usuarios internos.

El cortafuegos puede trabajar en tres niveles:

- *Al nivel de red,* controlando el trasiego de paquetes individuales (se denomina ***"apantallado"***).
- *Al nivel de aplicación,* controlando el acceso a servicios individuales (se denomina ***"proxy"***).
- *Al nivel de agente activo*, entrando a controlar el contenido de los accesos a los servicios (evitando virus, impidiendo el acceso a servicios de carácter no profesional, imponiendo límites al volumen de información en tránsito, etc.).

El cortafuegos debe tener características y capacidades distintas según trabaje en uno u otro nivel:

- *Volumen de tráfico* a gestionar, creciente desde el nivel de red al de aplicaciones que controlan el contenido, *"capacidad de control"* muy superior para el nivel de aplicación que para el nivel de red.
- *Registro de uso*: indiferenciado al nivel de red y con clasificación por servicios al de aplicación.
- *Identificación del usuario*: prácticamente imposible al nivel de red, pero posible al de aplicación (se llega a delegar en el cortafuegos toda la política de control de acceso, desde el exterior o el interior).

En definitiva, el cortafuegos consiste en un dispositivo informático (un enrutador o un ordenador) que separa físicamente un dominio de red de otro. Los enrutadores pueden controlar el tráfico en el nivel de red/transporte permitiéndolo o denegándolo selectivamente en base a la dirección fuente/destino y al número de puerto. Los ordenadores pueden controlar el tráfico en el nivel de aplicación. Los cortafuegos aplican un conjunto de operaciones de filtrado de paquetes del nivel red/transporte, tomando así decisiones de seguridad basadas en la información (dirección fuente y número de puerto), que proporcionan por ejemplo las cabeceras IP y TCP.

2.6.3. Cortafuegos a nivel de red

El propósito de este cortafuegos, también llamado de ***Filtrado de Paquetes,*** es proporcionar un punto de defensa y de acceso controlado y auditado para servicios, desde dentro y desde fuera de una red privada de la organización, permitiendo y/o denegando el flujo de paquetes a su través, con lo que proporciona control de acceso a dicha red.

Este cortafuegos suele materializarse por medio de un enrutador con filtros que proporcionan el control solicitado, utilizando reglas de filtrado de paquetes para conceder o denegar el paso de éstos al interior en base a la dirección fuente, a la dirección destino y al puerto. Ofrecen una seguridad mínima, pero su costo es muy bajo y pueden ser una alternativa apropiada para entornos de bajo riesgo. Son rápidos, flexibles y transparentes. Las reglas de filtrado no suelen poder mantenerse fácilmente en el enrutador, pero se dispone de herramientas para simplificar las tareas de crear y mantener esas reglas.

Los riesgos de los cortafuegos basados en el filtrado de paquetes son:

- El enrutador cuenta sólo con las direcciones origen y destino y los puertos contenidos en la cabecera del paquete IP para permitir o no el acceso de tráfico a la red interna. Un atacante tendrá acceso directo a cualquier equipo de la red interna una vez que el cortafuegos le haya concedido acceso.
- El enrutador no protege contra el *"spoofing"* engaño, de direcciones DNS ó IP.
- El enrutador proporciona poca o nula información útil de registro, *"logging"*.

Algunos cortafuegos de filtrado de paquetes no soportan la autenticación fuerte de usuarios.

El Cortafuegos de Filtrado de Paquetes no es aceptable para Entornos de Alto Riesgo (por ejemplo hospitales); ofrece una seguridad mínima para Entornos de Riesgo Medio (por ejemplo, Universidades); y puede ser la elección recomendable para Entornos de Bajo Riesgo.

2.6.4. Cortafuegos al nivel de aplicación

Estos cortafuegos ejecutan programas servidor denominados *proxies* (apoderados) que, como su nombre indica, tratan con los servidores externos de Internet, en nombre de clientes internos que solicitan servicios. O bien examinan las peticiones externas y las reenvían peticiones legitimas al servidor interno para que proporcione el servicio apropiado.

Estos cortafuegos se consideran más seguros que los simples filtros y ofrecen ventajas a una organización que tenga riesgos medio-altos como las siguientes:

- Este cortafuegos puede configurarse como la única dirección de ordenador visible para la red externa, requiriendo que todas las conexiones hacia/desde la red interna se realicen a su través.
- La utilización de *proxies* para los diferentes servicios impide el acceso directo de la red interna a servicios externos, protegiendo a la organización incluso contra la vulnerabilidad de los ordenadores internos mal configurados o no seguros.
- Este cortafuegos también soporta funciones de autenticación fuerte del usuario.
- Los *proxies* pueden proporcionar registro *(logging)* detallado en el nivel de aplicación. Los cortafuegos del nivel de aplicación deberían configurarse

- de modo que el tráfico de red externo aparezca como si lo originasen ellos (es decir, sólo el cortafuegos es visible para las redes externas). De esta forma, no está permitido el acceso directo a los servicios de red de la red interna y así mismo todas las peticiones entrantes para los diferentes servicios de red *(telnet, ftp, http, rlogin*, etc.) deben ir a través del *proxie* apropiado (uno por servicio) sin tener en cuenta cuál será el ordenador de la red interna destinatario final del servicio.

Si se requiere un servicio que no esté soportado por un proxy, se tienen tres posibilidades:

- Denegar el servicio Internet hasta que el fabricante del cortafuegos desarrolle un *proxy* seguro (alternativa preferida cuando los nuevos servicios poseen vulnerabilidades no aceptables).
- Desarrollar un *proxy* a medida (opción difícil que sólo puede emprenderse con técnicas sofisticadas).
- Pasar el servicio directamente a través del cortafuegos con un filtrado más reducido de paquetes, usando "configuraciones", lo que puede limitar algunas de las vulnerabilidades pero puede comprometer la seguridad de los sistemas internos situados tras el cortafuegos.

Cuando el servicio Internet no soportado por un *proxy* sea interno (dentro de la frontera de seguridad), también se pasa a través del cortafuegos, después que el administrador de éste defina el *plug* que permita el servicio pedido. Cuando esté disponible un *proxy* del fabricante del cortafuegos, se inhabilitará el *plug* y el *proxy* se hará operativo. Todos los servicios Internet internos deben procesarse por software *proxy* del cortafuegos. Si se pide un nuevo servicio, éste se denegará hasta que se disponga de un *proxy* del fabricante del cortafuegos y se verifique por el administrador del cortafuegos. Se puede desarrollar un *proxy* a medida por la propia organización o por otros fabricantes, pero sólo se podrá utilizar tras aprobarse por el responsable de seguridad.

2.6.5. Cortafuegos Híbridos

Muchos Cortafuegos combinan los tipos anteriores y los implementan en serie, lo que mejora la seguridad total, más que en paralelo, porque el perímetro de seguridad de red sólo será tan seguro como el menos seguro de los tipos utilizados.

La combinación híbrida depende de los servicios que requieran los usuarios y del nivel de riesgo que acepten. Por ejemplo el filtrado de paquetes maneja con más efectividad ciertos pret, SMTP) y los servidores *proxy* otros (FTP, WWW).

Cada tipo de cortafuegos puede asumir mejor unas u otras funciones. Así un enrutador puede asumir bien éstas dos:

- Gestión de direcciones. Internet tiene rangos de direcciones reservados para redes privadas. dichas redes no se anuncian públicamente y se aísla así efectivamente el encaminamiento, que queda reducido al nicho local. se utiliza un mecanismo de traducción dinámica de direcciones (NAT, *Network Address Translation*) para que se puedan establecer enlaces entre el interior y el exterior (habitualmente en ambos sentidos)
- *Cifrado de enlaces.* El dispositivo que actúa de cortafuegos tiene la ubicación idónea para establecer canales seguros de comunicaciones con otros cortafuegos remotos separados de aquél por redes no confiables.

Por su parte con un cortafuegos al nivel de aplicación ni se plantea la problemática de direcciones privadas aisladas pues no tiene canales directos y todo tiene que pasar por la aplicación proxy que hace de intermediario. Sin embargo la problemática de los canales cifrados entre aplicaciones se puede implantar cómodamente dentro de la funcionalidad *proxy,* lo que además puede eliminar el requerimiento de alterar las aplicaciones cliente y servidor en sí mismas.

En entornos de medio a elevado riesgo, un cortafuegos híbrido puede ser la elección ideal, Seria así la elección recomendada para Entornos de Alto Riesgo. una opción efectiva para los de Riesgo Medio; y una elección aceptable para los de Bajo Riesgo.

2.6.6. Amenazas a los cortafuegos

El cortafuegos se diseña para que sea el punto de ataque donde se concentren las amenazas. Un cortafuegos de nivel red/transporte puede estar sometido a dos grandes grupos de amenazas, unas genéricas y otras operacionales (o sea, referidas al entorno de las operaciones).

El ***Grupo de Amenazas Genéricas*** comprende las causadas por los siguientes agentes:

- Personas no autorizadas pueden ganar acceso lógico al cortafuegos.
- Personas no autorizadas de una red externa pueden suplantar a un sujeto de la red interna, llevando a cabo ataques de *spoofing*, "engaño", en direcciones de red, por ejemplo *spoofing.* IP desde una conexión de red a otra, atravesando el cortafuegos.

- Personas no autorizadas pueden realizar ataques a los servicios siempre que puedan ser accedidos desde fuera de la red interna. Las amenazas específicas encontradas dependen de los protocolos que se permiten pasar a través del cortafuegos.
- Personas no autorizadas pueden realizar ataques de encaminamiento fuente en el nivel de red. Varios protocolos del nivel de red permiten al emisor de un paquete especificar el camino que el paquete seguirá desde la fuente al destino; si el encaminamiento fuente está indicado en la cabecera de protocolo, la función que procesa éste se saltará cualquier comprobación de reglas, ofreciendo así un camino no deseado para cruzar "por un túnel" el cortafuegos.
- Personas no autorizadas pueden realizar intentos de penetración no detectados (si no existe personal en la red atacada que se dé cuenta de que tales ataques están teniendo lugar).
- Un atacante puede no ser detectado mientras realiza intentos de penetración repetidos si falta revisión del registro o de los datos de auditoría, bien por la cantidad de datos generados o por falta de herramientas de revisión adecuadas.
- Un atacante puede modificar/degradar el registro de auditoría, bien directamente manipulándolo a través de un interface del cortafuegos. Como un protocolo de control específico soportado por la red, bien enmascarando sus acciones (por ejemplo averiando el cortafuegos tras realizar una penetración o intento para que pueda perderse el registro de auditoria si no está bien protegido).
- Un atacante puede modificar la configuración del cortafuegos y otros datos de seguridad relevantes (esta amenaza es similar a la anterior, salvo que los datos que dice un atacante son esa configuración y otros datos de seguridad críticos).
- Ciertos defectos en el cortafuegos pueden generar brechas de seguridad que los agentes amenazadores pueden descubrir por accidente o búsqueda dirigida y utilizar para trastornar el funcionamiento de las funciones de seguridad y cambiarlas en su provecho (tanto en la entrega e instalación del cortafuegos como durante su funcionamiento normal, con métodos de "minado" de las funciones de seguridad).

El ***Grupo de Amenazas aplicadas al Entorno de Operación*** implican las causantes de riesgos potenciales del sistema por el entorno o por medios procedimentales como:

- Personal de administración del sistema descuidado, negligente o intencionalmente hostil puede saltarse fácilmente los mecanismos de

- seguridad del cortafuegos puesto que es responsable de establecer las reglas de control de acceso y de monitorizar el registro de auditoria.
- Ciertos usuarios de una red protegida (situados detrás del cortafuegos) pueden querer compartir información con usuarios de la red externa, enviando información de forma ilegítima a sabiendas que este tipo de cortafuegos generalmente será inefectivo contra esta clase de ataques pues está diseñado específicamente para proteger las redes internas de las redes externas sin tratar de comprobar el contenido del paquete.
- Ciertos usuarios de una red protegida pueden atacar máquinas de esta red protegida, sin que el cortafuegos las pueda proteger, al no ser un ataque a información que pase por el cortafuegos.
- Ciertos usuarios de una red protegida pueden realizar ataques sofisticados a los servicios y protocolos de alto nivel, eligiendo defectosde los niveles de protocolo (y los servicios que utilizan dichos protocolos) por encima del nivel de transporte: el cortafuegos puede denegar el paso de paquetes a servicios específicos, pero una vez que los permite pasar, no les defiende de posibles ataques a los servicios elegidos, pues no verifica el contenido del paquete.

En un entorno operacional con cortafuegos de filtrado de paquetes del nivel red/transporte, se asumen condiciones de utilización segura de diverso tipo: (físicas, de personal, de conectividad).

Condiciones físicas:

- El cortafuegos y la consola asociada directamente conectada son seguros: es decir, su acceso se limita sólo al personal autorizado. El personal autorizado de administración interactúa con el cortafuegos sólo a través de consolas directamente conectadas, es decir, no se permite ningún "login de red" a los administradores. El cortafuegos no requiere para funcionar cambios de las propiedades operativas (por ejemplo, aplicaciones de software, hardware) de la red interna o de la red externa,

Condiciones de tipo personal:

- El cortafuegos sólo está diseñado para actuar como tal y no para proporcionar servicios adicionales de usuario (por ejemplo, *"login"*) a cualquiera de la red interna o externa. Sólo los administradores poseen acceso directo. Se supone que los administradores no son hostiles y son de confianza para realizar sus funciones correctamente.

Condición de tipo de conectividad:

El cortafuegos es el único dispositivo de interconexión entre las redes. No se permite una configuración con dos redes, una pública y otra privada, conectadas a la vez por un cortafuegos y por una conexión directa.

2.6.7. Políticas de seguridad para instalar un Cortafuegos

Hay que especificar los siguientes extremos:

- Se identifica cada "isla" de seguridad (o sea una red físicamente diferenciable a la que se aplica una política de seguridad sea única o común para todos los equipos con un mínimo de excepciones).
- Tras identificar varias islas, se decide si se dispone cortafuegos entre ellas y se determina la política de tránsito (lo habitual es prohibir todo tipo de tránsito entre redes y sólo autorizar explícitamente los flujos permisibles). Si no hay tráfico entre dos islas, no se requiere cortafuegosentre ellas. Si el tráfico entre ambas es voluminoso, se puede justificar un cortafuegos explícitamente dedicado a esta interfaz. Es habitual disponer varias islas de seguridad en forma de estrella alrededor de un cortafuegos único con varias puertas (cortafuegos que suele estructurarse internamente como multinivel). Esta estructura en estrella no puede convertirse en cuello de botella ni limitar el número de niveles de defensa en profundidad.
- Tras determinar la arquitectura (topología y nivel de actuación del cortafuegos) hay que plasmar la política de seguridad explicitando los flujos permitidos de información y las condiciones de autorización para cada uno de esos flujos.
- Se especifica el responsable de diseñar y mantener dicho plan de seguridad, de implantar las reglas pertinentes y de gestionarla (dando altas y bajas de rutas y de Servicios).
- Se diseña una batería de pruebas que permita verificar la operación correcta del cortafuegos con pruebas de caja negra (verificación global de servicios) y de caja blanca (satisfacción de cada una de las reglas individuales), corren las pruebas y valida la implantación. Se ejecutarán pruebas de regresión cada vez que se altere la configuración: nueva política, nuevas reglas, eliminación de reglas, cambio del equipo o de versión de *software* o *firmware*, etc.
- Se registran todas las actuaciones en el libro de operación del sistema, junto con los resultados de la aplicación de la batería de pruebas. Hay que disponer de varios planes: de registro de actividad del cortafuegos de respuesta a incidencias, de contingencia.
- Se identifican el/los responsable/s de prestar atención a las alarmas que se produzcan

2.6.8. Autentificación e Integridad de la información de configuración en los cortafuegos

Los cortafuegos basados en enrutador no proporcionan autenticación de usuario. Los cortafuegos de tipo *proxy* pueden proporcionar las siguientes categorías de autenticación:

- Uso de *"username/password"*, la menos robusta pues puede monitorizarse usando *sniffers*.
- Uso de OTPs *(One-Time Passwords),* con *tokens* software ó hardware que generan una nueva palabra de paso para cada sesión (como no se pueden reutilizar las palabras de paso anteriores se reduce el riesgo si se monitorizan (utilizando *sniffers),* pierden, prestan o roban.
- Uso de "Certificados Digitales" que involucran Autoridades de Certificación y permiten firmar electrónicamente aplicando algoritmos de cifrado de clave pública, por ejemplo RSA.

Para impedir modificaciones no autorizadas de la configuración del cortafuegos, se debe utilizar alguna forma de proceso que garantice la integridad de su información. La decisión de permitir o denegar a un paquete su paso a través del cortafuegos se basa en atributos del sujeto, del objeto, de la información de estado generada por el cortafuegos y de las reglas de control de acceso configuradas administrativamente. Normalmente se realizan checksums **CRC** *(Ciclic Redundancy Checks)* o funciones *hash* criptográficas (por ejemplo, MD5) de la imagen *run-time* (en tiempo de ejecución) y se guardan en medios protegidos. Cada vez que modifica la configuración del cortafuegos un individuo autorizado (normalmente el administrador del cortafuegos) se ha de actualizar la base de datos "en-linea" de integridad del sistema y guardarla en un sistema de ficheros en la red o en soporte removible. Si la comprobación de la integridad del sistema muestra que los ficheros de configuración del cortafuegos se han modificado, se avisará que el sistema ha visto comprometida su seguridad. La base de datos de integridad del sistema del cortafuegos se actualizará cada vez que se modifica la configuración del cortafuegos. Los ficheros de integridad del sistema deben guardarse en soporte de sólo lectura o de almacenamiento "fuera de linea". El administrador debe comprobar regularmente la integridad del sistema obteniendo un listado de todos los ficheros que se han modificado, reemplazado o borrado. Es importante que los procedimientos operacionales y sus parámetros de configuración se encuentren documentados, actualizados y guardados en lugar seguro a salvo.

2.6.9. Alternativas en el contrafuegos: encaminar frente a reenviar

La política de seguridad de un cortafuegos es diferente si actúa como un enrutador o como un reenviador *proxy* de paquetes Internet. Un cortafuegos basado en un enrutador, al actuar como un dispositivo de filtrado de paquetes, no tiene más opción que encaminar paquetes. En un cortafuegos del nivel de aplicación todas las conexiones internas y externas deben realizarse a través de *proxies* de aplicación, sin encaminar ningún tráfico entre interfaces de las redes interna y externa que puedan saltar los controles de seguridad, como permiten estos dos mecanismos..

Encaminamiento fuente. En este mecanismo de encaminamiento, la fuente, no los enrutadores intermedios, determina el camino a una máquina destino. El encaminamiento fuente se utiliza principalmente para depurar problemas de red pero también permite ataques a un ordenador. Si un atacante conoce alguna de las conexiones seguras entre sus ordenadores, el encaminamiento fuente se puede usar para aparentar que los paquetes dañinos vienen de un ordenador confiable. Esta amenaza puede neutralizarse fácilmente, configurando unenrutador de filtrado de paquetes para rechazar los que contienen la opción de encaminamiento.

De este modo una organización que desea evitar el problema del encaminamiento fuente escribirá una política de seguridad consistente en eliminar paquetes de encaminamiento fuente.

"Spoofing IP". Este enmascaramiento del atacante que hace pasar su maquina como un ordenador de la red destino (engañando a una máquina destino con que los paquetes vienen de una máquina confiable de la red interna destino) exige especificar claramente la política de seguridad que trata el encaminamiento de paquetes. El *spoofing* IP utiliza diversas técnicas para trastornar el control de acceso basado en IP suplantando a otro sistema utilizando su dirección IP. Para protegerse contra los ataques de spoofing IP, la autenticación basada en direccionamiento fuente ha de combinarse con otro esquema de seguridad.

2.6.10. Arquitecturas de cortafuegos

Los cortafuegos se pueden materializar en diferentes arquitecturas que proporcionan diversos niveles de seguridad con diferentes costos de instalación y operación. Las organizaciones deben hace corresponder su perfil de riesgo con el tipo de arquitectura de cortafuegos seleccionada. Las principales arquitecturas de cortafuegos son:

- El cortafuegos con ***ordenador multi-puerto (multi-homed host)*** tiene más de una interfaz de red (dos es el caso más común). Cada interfaz se conecta a segmentos de red física lógicamente separados. Un cortafuegos de doble puerto tiene dos tarjetas de red (NTC, *Network Interface Cards) y* cada interfaz conecta a una red diferente. Para impedir que el tráfico de paquetes IP procedente de la red no segura se encamine directamente a la red segura y no a través del cortafuegos que actúa como intermediario, incluso se inhabilitará el encaminamiento del cortafuegos.
- El cortafuegos con ***ordenador pantalla (screened host)*** utiliza obliga a conectar todos los ordenadores de fuera a un ordenador denominado "bastión", en vez de permitir su conexión directa a otros ordenadores internos menos Seguros. Para realizarlo, se configura el enrutador de filtrado de paquetes para que todas las conexiones a la red interna desde la red externa se dirijan al ordenador "bastión"
- El cortafuegos con ***subred pantalla (screened subnet)*** tiene una arquitectura similar a la del "ordenador pantalla", pero le añade una capa extra de seguridad creando una red denominada "perimetral" que reside en el ordenador "bastión" y se encuentra separada de la red interna. Se crea una "subred pantalla" añadiendo una red perimetral que separe la red interna de la externa. Si existe un ataque con éxito en el ordenador bastión, el atacante está restringido a la red perimetral por el "enrutador pantalla" que se conecta entre la red interna y la red perimetral.

2.6.11. Mecanismos de respaldo en cortafuegos

El cortafuegos, al igual que cualquier sistema de la red, debe tener alguna política que defina su respaldo o *backup* para conseguirla recuperación tras un fallo o un desastre natural. Así mismo los ficheros de datos y los de configuración del sistema necesitan tener algún plan de respaldo en caso de fallo del cortafuegos.

El cortafuegos y el conjunto del sistema que dependen de él (software, datos de configuración, ficheros de base de datos, etc.) deben contar con sistemas de respaldo, por ejemplo un proceso de copias de seguridad periódico (cada pocas horas, a diario, semanalmente, mensualmente, etc.), cuyas copias deben almacenarse de forma segura en un soporte de sólo lectura para que los datos no se sobrescriban inadvertidamente y deben protegerse para que el soporte sólo sea accesible por el personal apropiado.

Otra alternativa de respaldo consiste en tener un mecanismo de tolerancia a fallos llamado "replicación del cortafuegos de grado dos", es decir otro

cortafuegos configurado como el primero y guardado de forma segura para que en caso de fallo del actual, el cortafuegos de respaldo se conmute automática o manualmente mientras se repara el averiado. Con esta alternativa la degradación del servicio es menor, pero a costa de un mayor coste por la duplicidad del cortafuegos y el mecanismo de conmutación.

Toda la administración del cortafuegos se debe realizar desde el terminal local, cuyo acceso físico debe limitarse sólo al administrador del cortafuegos y al administrador de respaldos. No debe permitirse ningún acceso remoto al software operativo del cortafuegos. Este nunca debe utilizarse como servidor de propósito general y sólo debe contener como cuentas de usuario las del administrador del cortafuegos y las del administrador de respaldos o copias de seguridad.

2.6.12. Cortafuegos para Intranets y con capacidad VPN

Aunque los cortafuegos se colocan habitualmente entre una red corporativa y la red no segura del exterior (Internet), se utilizan a menudo en grandes organizaciones para crear subredes distintas dentro de la Intranet. Un cortafuegos para Intranet permite aislar una subred o segmento de red particularde la red corporativa total (por ejemplo la del departamento de nóminas o de contabilidad de la organización), con dos objetivos posibles:

- Evitar que todos los usuarios internos puedan acceder a la información de la subred guardada, (que estará disponible sólo para los que la tengan que manejar por necesidad)
- Conseguir un alto grado de responsabilidad en el acceso y utilización a subsistemas con información sensible, confidencial o crítica para la organización, con un control de acceso fuerte que soporte auditoria y registro.

Estos sistemas y controles deberían utilizarse para dividir la red corporativa interna a la hora de soportar políticas de acceso desarrolladas por los propietarios de información designados.

Por otra parte, las llamadas redes privadas virtuales o VPN *(Virtual Private Networks)* permiten a redes seguras comunicarse con otras redes seguras apoyándose en redes no seguras como Internet. Puesto que algunos cortafuegos proporcionan esta "capacidad VPN', es necesario definir una política de seguridad para establecer dichas VPN. Cualquier conexión entre cortafuegos por medio de redes públicas habrá de utilizar VPN cifradas para asegurar la confidencialidad y la integridad de los datos que pasan a través de la red

pública. Todas las conexiones VPN deben ser aprobadas y gestionadas por el administrador de servicios de red, quien debe establecer los medios apropiados para distribuir y mantener claves de cifrado antes del uso operacional de los VPN.

2.6.13. Configuración de cortafuegos como servidor DNS

En Internet, el DNS *(Domain Name Service)* proporciona la correspondencia y la traducción de los nombres de dominio a direcciones IP. Algunos cortafuegos se pueden configurar como servidores DNS de distintos niveles (primarios, secundarios o caché).

Debe observarse que no suele ser una decisión del ámbito de la seguridad la forma de gestionar los servicios DNS. Muchas organizaciones utilizan para gestionar su DNS una "tercera parte", un ISP *(Internet Service Provider):* en este caso, el cortafuegos puede utilizarse como un servidor DNS caché que mejora el rendimiento pero que no necesita mantener su propia base de datos DNS. Si la organización decide gestionar su propia base de datos DNS, puede ser ventajoso que el cortafuegos actúe como servidor DNS, pero en este caso es necesario tomar otras precauciones de seguridad. Así, si se implementa como servidor DNS, el cortafuegos puede configurarse para ocultar la información de los ordenadores internos de la organización: o sea, los ordenadores internosobtienen una visión no restrictiva de los datos DNS internos y externos, mientras que los ordenadores externos no tienen acceso a la información relativa a las máquinas internas. Para el mundo exterior, todas las conexiones a cualquier ordenador de la red interna parecerán haberse originado desde el cortafuegos. Con la información sobre los ordenadores internos oculta desde el exterior, un atacante no sabrá los nombres y direcciones de los ordenadores internos que ofrecen servicios a Internet. Por tanto una posible política
de seguridad para ocultar el DNS puede consistir en que el cortafuegos opere como un servidor DNS y se configure para ocultar la información relativa a la red interna al mundo exterior (Internet).

2.7. IP V.6

El desarrollo de la versión 6 de IP, IPv6, llamada también IP de siguiente generación, se ha visto estimulado por la urgente necesidad de resolver los problemas de direcciones de Internet, encaminamiento, rendimiento, seguridad y congestión. Para más detalles, se pueden consultar las RFC más recientes. En la RFC 1884 se describen las direcciones de IPv6 y la RFC 1883 describe el protocolo versión 6. La RFC 1885 describe ICMPv6 y en la RFC 1886 se trata sobre las extensiones y el Sistema de nombres de dominio. En la RFC 1887 se propone una arquitectura para la asignación de nombres.

2.7.1. Descripción general de IPv6

Las características de IPv6 son las siguientes:

- Dispone de direcciones de 128 bits, 16 octetos, que se pueden estructurar jerárquicamente para simplificar la delegación de direcciones y el encaminamiento.
- Simplifica la cabecera principal de IP, pero define muchas cabeceras de extensión opcionales. De esta forma se pueden incorporar las nuevas funciones de intercomunicación cuando se necesiten.
- Dispone de autentificación, integridad de datos y confidencialidad en el nivel de IP.
- Introduce flujos, que se pueden utilizar para disponer de nuevos tipos de requisitos de transmisión, como el vídeo en tiempo real.
- Facilita el encapsulado de otros protocolos y proporciona un mecanismo de control de congestión cuando transporta protocolos «extraños».
- Proporciona nuevos métodos de autoconfiguración automática de direcciones e incorpora una comprobación de que las direcciones son únicas.
- Mejora el descubrimiento de encaminador y la detección de encaminadores fuera de servicio o vecinos inalcanzables por un enlace.
-

2.7.2. Terminología

La versión 6 realiza ciertos cambios de nomenclatura respecto a la versión 4 e introduce algunos nuevos términos:

- Un paquete es una cabecera de IPv6 más una carga útil.
- Un nodo es cualquier sistema con IPv6.
- Un encaminador es un nodo que reenvía paquetes de IPv6 que no son para él.
- Un enlace es un medio por el que se comunican los nodos usando la capa de enlace.
- Vecinos son los nodos conectados a un mismo enlace.

El término paquete es uno de los que más se ha abusado en el mundo de las redes. Se usa para describir las unidades de datos del protocolo (PDU) de la capa de enlace, hasta la capa de aplicación. ¿Por qué en Ipv6 se ha cambiado el nombre de datagrama por paquete? Una de las innovaciones de IPv6 es que se puede utilizar para transportar tráfico de otros muchos protocolos y, por tanto,

su carga útil puede que no fuese una PDU del grupo de TCP/IP. Cuando la PDU es de IP, sigue siendo apropiado el término datagrama.

2.7.3. Direcciones IPv6

Las direcciones de IPv6 tienen 16 octetos (128 bits). La notación usada es bastante compacta, representándose como ocho números hexadecimales, separados por dos puntos. Cada número en hexadecimal representa 16 bits. Por ejemplo:

41BC:0:0:0:5:DDE1:8006:2334

Vemos que se pueden eliminar los ceros de la izquierda de un campo (por ejemplo, se pone 0 en lugar de 0000 o 5 en lugar de 0005). El formato se puede comprimir aún más eliminando una serie de campos a 0 por::. Por ejemplo:

41BC::::5:DDE1:8006:2334

Se han eliminado tres grupos y por tanto :::: representa la cadena :0:0:0:.

Por último, a veces las direcciones de la versión 4 de IP se insertan en los últimos 4 octetos de las direcciones de la versión 6. Se puede escribir usando un formato de direcciones que utiliza tanto la notación punto como la de dos puntos, como:

0:0:0:0:0:FFFF: 128.1.35.201

2.7.3.1. Asignación de direcciones

Con un espacio de direcciones de 128 bits hay sitio para muchos tipos diferentes de direcciones. como:

- Proveedores jerárquicos de servicios según una dirección de unienvio global.
- Direcciones geográficas jerárquicas de unienvio globales.
- Direcciones privadas para uso exclusivo dentro de una organización.
- Direcciones locales y globales de unienvio.

La versión 6 no usa difusión. si no que utiliza el multienvio para funciones de control como la resolución de direcciones y el arranque. La razón es que la difusión de un mensaje interrumpe a todos los dispositivos de un enlace. En la mayoría de las ocasiones sólo unos pocos dispositivos necesitan realmente examinar el mensaje. Además, al restringir los mensajes de control de la versión

6 a direcciones de multienvio se evita que haya interferencias entre las versiones 4 y 6 cuando comparten un mismo enlace.

2.7.3.2. Asignación completa de direcciones

La Autoridad de asignación de números de Internet (IANA - Internet Assigned Numbers Authority) tiene la tarea de asignar direcciones de IPv6 a las organizaciones regionales de registro repartidas por el mundo. Estas últimas pueden, a su vez, asignar de direcciones a regiones menores, a registros nacionales o a proveedores de servicios.

En la siguiente tabla se muestra el plan sugerido de asignación del espacio de direcciones.

Asignación	Fracción del prefijo (binario)	Espacio de direcciones
Reservado	0000 0000	1/256
No asignado	0000 0001	1/256
Reservado para la asignación del NSAP	0000 001	1/128
Reservado para la asignación de IPX	0000 010	1/128
No asignado	0000 011	1/128
No asignado	0000 1	1/32
No asignado	0001	1/16
No asignado	001	1/8
Direcciones unienvio para proveedores	010	1/8
No asignado	011	1/8
Direcciones unienvio geográficas	100	1/8
No asignado	101	1/8
No asignado	110	1/8
No asignado	1110	1/16
No asignado	1111 0	1/32
No asignado	1111 10	1/64
No asignado	1111 110	1/128
No asignado	1111 1110 0	1/512
Direcciones de uso por el enlace local	1111 1110 10	1/1024
Direcciones para uso local	1111 1110 11	1/1024
Direcciones de multienvio	1111 1111	1/256

- Se usa un gran bloque para el direccionamiento a través de proveedores de servicios. Existen bloques para LAN independientes o lugares

- completos que no estén conectados a Internet, de manera que pueden asignarse sus propias direcciones.
- Se han asignado bloques para las direcciones de IPX y para las direcciones de Puntos de acceso al servicio de red de OSI (NSAP).
- Se ha reservado un gran bloque para las direcciones geográficamente distribuidas.

En la actualidad. casi las tres cuartas partes del espacio de direcciones no tiene asignado ningún uso.

2.7.3.3. Prefijo del formato de las direcciones

Los primeros bits de una dirección, llamados Prefijo de formato (Format Prefix) identifica el tipo de dirección. Por ejemplo, el prefijo 010 indica las direcciones de unienvio asignadas a proveedores de servicios. Como es de suponer, el formato del resto del espacio de direcciones depende del prefijo de formato.

2.7.3.4. Direcciones para proveedores

Actualmente se propone una estructura jerárquica simple para las direcciones para proveedores:

3 bits	m bits	n bits	o bits	125-m-n-o bits
010	ID de registro	ID Proveedor	ID cliente	Dentro de cliente

Vemos que resulta sencillo encaminar el tráfico a un proveedor comparando la primera parte de la dirección con las entradas de la tabla de encaminamiento. El proveedor, a su vez, puede encaminar el tráfico a sus clientes comparando un trozo mayor de la dirección con sus entradas en la tabla de encaminamiento. Cuando se usa este formato, la organización cliente poseerá el espacio de direcciones suficiente para crear una jerarquía interna apropiada. Una organización puede estructurar su espacio de direcciones en subredes y host, como en la actualidad, o podría añadir algunos niveles jerárquicos adicionales. Por ejemplo, se podría usar una jerarquía consistente en área, subred y host.

En la versión 6 no están prohibidas las direcciones con todos los bits a cero o a uno.

2.7.3.5. Direcciones para lugares independientes

En la actualidad, para una LAN o una red que no está conectada a Internet se usa un bloque especial de direcciones, como la 10.0.0.0 o la 172.16.0.0, reservadas con este objetivo. Pero si la organización necesita posteriormente conectarse al mundo externo, tiene que realizar un gran esfuerzo de reconfiguración. La versión 6 ha tenido en cuenta este problema de reasignación de forma mucho mas elegante, como veremos mas adelante.

2.7.3.5. Direcciones de enlace local

Recordemos que un enlace es un elemento de comunicaciones, como una Ethernet 2 (Nota: Para IPv6 se ha definido un nuevo código de tipo de Ethernet, el X'86-DD), TokenRing, una red de fibra óptica (FDDI), una red de retransmisión de tramas, una red de Modo de transferencia asíncrono (ATM) o una línea punto a punto. Resulta sencillo automatizar las direcciones de un enlace aislado sin conexión con un encaminador. Las direcciones de enlace local tienen la forma:

1111111010 (10 bits) 00... 00	Dirección única para la tecnología del enlace

Por ejemplo si el enlace es una LAN:

1111111010 (10 bits) 00... 00	Dirección MAC de la LAN

Una dirección de enlace local también es útil durante la inicialización.

2.7.3.7. Direcciones locales

Un lugar con encaminadores pero sin conexión con un proveedor de servicios. puede generar automáticamente direcciones internas de la forma:

1111111011 (10 bits) 00... 00	ID de subred Dirección única para la tecnología de enlace

Los encaminadores se dan cuenta del prefijo (incluyendo el ID de subred) en el enlace.

Vemos lo sencillo que es migrar a una conectividad de proveedor de servicios. Tan sólo hay que configurar el encaminador con un nuevo prefijo que incluye elRegistro el proveedor de servicio y los números de cliente junto con los números de subred. El encaminador se dará cuenta del nuevo prefijo y los host empezarán a utilizarlo. No será necesario modificar ninguna parte de las direcciones asignadas al lugar.

2.7.3.8. Formato de las direcciones de Multienvio

En la versión 6 las direcciones de multienvio tienen una definición más clara y flexible que las direcciones de multienvio de la versión 4. Existen muchos tipos diferentes de direcciones de multienvio. Tiene elementos iniciales diferentes para diferenciar si la dirección es permanente o temporal, local o global.

Las direcciones de multienvio tienen el formato:

8 bits	4	4	112 bits
11111111	000T	Ámbito	ID de grupo

T=0 para una dirección permanente de multienvio pública.
T=1 para una dirección temporal de multienvio.

Los códigos de ámbito indican si el ámbito es el mismo nodo, un enlace local, el lugar la organización o global. El ámbito del mismo nodo incluye el caso en que un cliente envía un mensaje de multienvio a servidores situados en el mismo host. Los códigos concretos de ámbito son:

0 reservado
1 ámbito local al nodo
2 ámbito local al enlace
3 no asignado
4 no asignado
5 ámbito local al lugar
6 no asignado
7 no asignado
8 ámbito local a la organización
9 no asignado
A no asignado
B no asignado
C no asignado
D no asignado
E ámbito global

E reservado
F reservado

2.7.3.9. Direcciones de envió a uno

Se ha propuesto un nuevo tipo, experimental, de direccionamiento, el direccionamiento de envío a uno (anycast). Una dirección de envío a uno es una dirección de unienvio asignada a más de una interfaz. Inicialmente. sólo los encaminadores podían tener direcciones de envío a uno. Por ejemplo una dirección de envío a uno podría identificar:

- Todos los encaminadores de un proveedor de servicios concreto.
- Todos los encaminadores de la frontera de un Sistema autónomo dado.
- Todos los encaminadores conectados a una determinada LAN.

Se puede incluir una dirección de envío a uno en una ruta de origen. Significa «Usa el encaminador más cercano con esta dirección de envío a uno». Por ejemplo. si la dirección de envío a uno identifica los encaminadores de un proveedor de servicios. se podría usar para decir «Accede a este proveedor de servicio usando el camino más corto». Por supuesto, una Interfaz de encaminador que dispone de una dirección de envío a uno también tiene su propia dirección real.

2.7.4. Direcciones especiales

Existen varios formatos de direcciones especiales en IPv6.

2.7.4.1. Direcciones sin especificar

La dirección con todo ceros

0:0:0:0:0:0:0:0

significa «dirección sin especificar» (unspecified address). A veces se utiliza como origen durante la inicialización, cuando un sistema todavía no conoce su propia dirección.

2.7.4.2. Bucle interno en la versión 6

La dirección de bucle interno (loopback) de la versión 6 es:

0:0:0:0:0:0:0:1

2.7.4.3. Direcciones de la versión 4

En un entorno con mezcla de versión 4 y 6, las direcciones de los sistemas de IP versión 4 que no admiten la versión 6 se traducen en direcciones de la versión 6 de la forma:

0:0:0:0:0:FFFF:a.b.c.d

donde a.b.c.d es la dirección original de IP.

2.7.4.4.Direcciones de la versión 6 que interactúan con la versión 4

Se usa otro formato especial para los nodos de la versión 6 que se comunican con otros a través de una red intermedia de la versión 4. Se denomina encapsulamiento (tunneling) de IPv4.

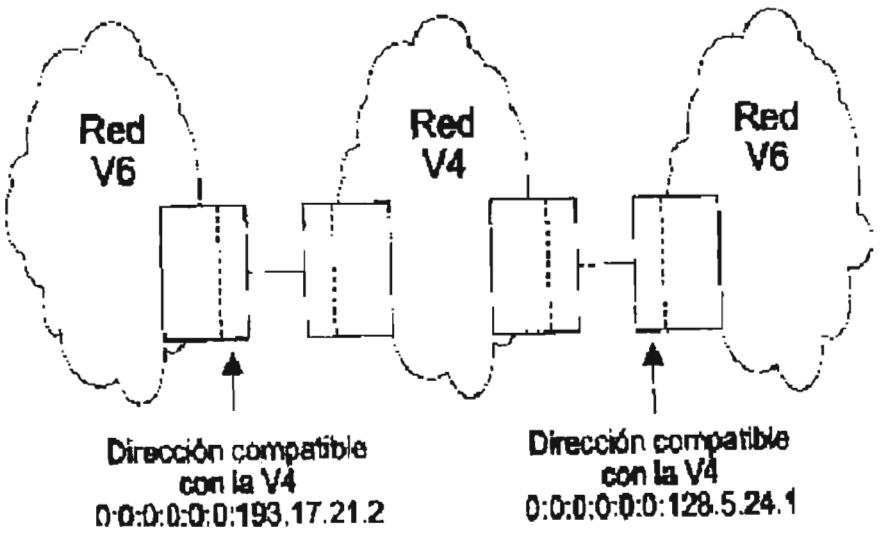


Fig 55. Direcciones de IPv6 compatibles con IPv4.

Figura 2.43 Direcciones de IPv6 compatibles con IPv4

Como se muestra en la Figura 2.43, las interfaces de la frontera deben tener direcciones de la versión 4. Se hacen corresponder con direcciones de IPv6 especiales con un formato compatible con iPv4:

0:0:0:0:0:0:a.b.c.d

Por tanto, existe una relación sencilla entre las representaciones de la versión 4 y la versión 6.

2.7.5. Formato de la cabecera IPv6

La cabecera básica es muy simple, como se muestra en la Figura 2.44. Vemos que existen muy pocos campos:

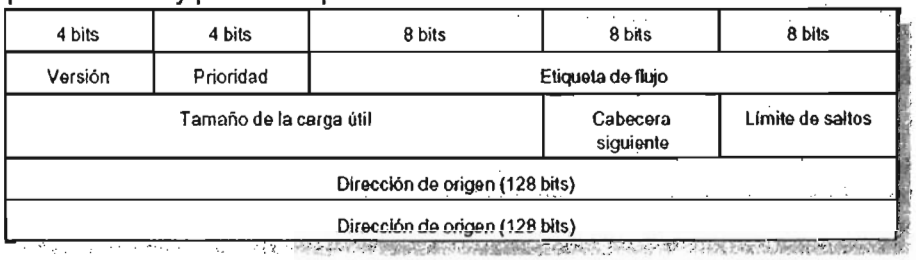


Figura 2.44

Versión — Es 6 para IP siguiente generación

Prioridad — Diferencia el tráfico interactivo del flujo, o define la posibilidad de descarte durante la congestión.

Tamaño de la carga útil — (l6 bits) Si el tamaño es menor o igual a 64 Kilobits, este campo indica el tamaño de la parte del paquete que sigue a la cabecera inicial de IPv6. Si el tamaño es mayor de 64 Kilobits, se pone el tamaño de carga útil a cero y el tamaño real se indica en una opción carga útil extra (Jumbo payload) de una cabecera posterior.

Limite de saltos — Se decrementa en uno en cada encaminador. Si el valor llega a cero el paquete se descarta.

Siguiente cabecera — Indica el tipo de cabecera de protocolo que sigue, por ejemplo, 6 para la cabecera de TCP.

Etiqueta de flujo — Indica que el tráfico necesita un tipo especial de tratamiento, por ejemplo, vídeo en tiempo real

2.7.5.1. Prioridad

El campo prioridad tiene una doble función. Para el tráfico de TCP con control de congestión, asigna números altos a los paquetes de control y al tráfico interactivo y números bajos al tráfico en bruto

Concretamente, los valores son:

0 Tráfico sin caracterizar.
1 Tráfico de «relleno». por ejemplo, las noticias de red.
2 Transferencia de datos sin atención, por ejemplo, el correo electrónico.
3 Reservado.
4 Transferencias de datos atendidas, por ejemplo, transferencias de archivos.
5 Reservado.
6 Tráfico interactivo, por ejemplo, telnet.
7 Tráfico de control de Internet, por ejemplo, protocolos de encaminamiento.

IPv6 se puede usar para transmitir tráfico de ISO, DECnet y otros. Los valores de prioridad entre 0 y 7 se pueden usar con cualquier protocolo que imponga su propio control de flujo.

Los valores del 8 al 15 se usan como mecanismo de control de congestión cuando un protocolo, por ejemplo, UDP o IPX, no imponen su propio mecanismo de control de congestión. Cuando la red se congestiona, el tráfico se descarta. Es peor descartar unos tipos de datos de aplicaciones que otros. Valores bajos, como 8 o 9 significa que ese paquete es más adecuado para descartar.

2.7.5.2. Uso de la etiqueta de flujo

Un flujo es una secuencia de paquetes desde un origen a un destino que necesita cierto tratamiento especial. Por ejemplo. la voz o el video en tiempo real requieren distinto tratamiento que la transferencia masiva de datos.

La etiqueta de flujo se usa para identificar un flujo de datos que tiene un mecanismo de manejo especial, como por ejemplo la reserva de ancho de banda.

El que unos paquetes pertenezca a un flujo se indica poniendo una etiqueta de flujo distinta de cero. Los paquetes que pertenecen a un flujo concreto tienen los mismos datos de dirección de origen, dirección de destino, prioridad y etiqueta de flujo.

2.7.6. Extensión de cabecera de IPv6

El uso de extensión de cabeceras es una idea innovadora que permite añadir funcionalidad incrementalmente a la versión 6 de IP.

En la cabecera de la versión 4 de IP, se usaba el campo proveedor para indicar qué tipo de cabecera seguía a la cabecera de IP. por ejemplo TCP o UDP. La versión 6 usa un campo siguiente cabecera más general. Si la siguiente cabecera es una cabecera de TCP o de UDP. el valor del campo siguiente cabecera vale 6 o 17, el identificador de protocolo de TCP o de UDP.

Pero algunas extensiones de cabecera se pueden colocar entre la cabecera de IPv6 y una cabecera de mayor nivel. Se usan para opciones, como las de ruta de origen o las de seguridad. La fragmentación también se ha trasladado a una extensión de cabecera.
Como se muestra en la figura anterior, cada una de las extensiones de cabecera contiene un campo Siguiente cabecera de manera que las cabeceras se van encadenando. Por último, en la última extensión de cabecera se identifica el protocolo de la siguiente capa.
Este esquema proporciona una gran flexibilidad. Se pueden definir nuevas opciones en cualquier

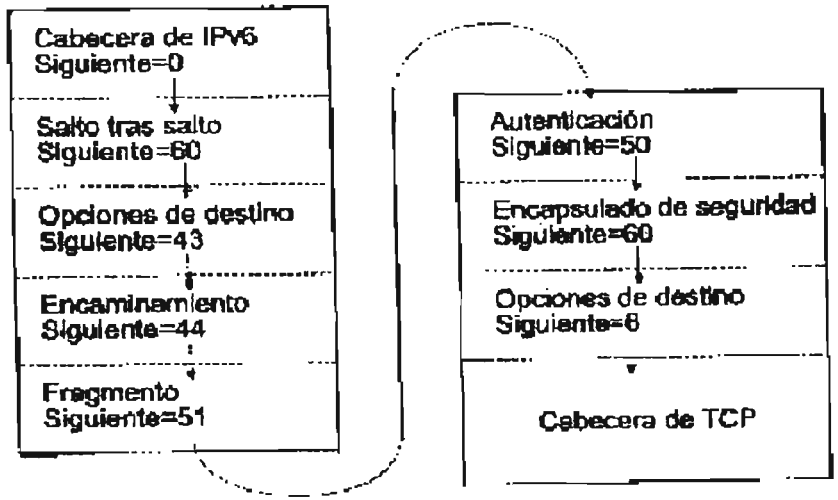


Fig.58. Extensiones de cabeceras

Figura 2.45 Extensiones de cabeceras

momento según se necesiten y no se necesita restringir su tamaño. Tengamos en cuenta también, que la última extensión de cabecera puede apuntar a una cabecera que pertenece a un grupo de protocolos completamente diferente, como por ejemplo, ISO o DECnet.
En la siguiente tabla se muestran los identificadores definidos actualmente. Algunas cabeceras contienen información que se debe procesar en todos los nodos de la ruta, mientras que otras contienen información que sólo se necesita procesar en el destino.

Cabecera	Número en el campo «siguiente cabecera» anterior
Opciones de salto a salto	0
Opciones de destino	60
Encaminamiento	43
Fragmentación	44
Autenticación	51
Encapsulado de seguridad de la carga útil	50
Sin siguiente cabecera	59

El orden que se muestra en la Figura 2.45 refleja el orden recomendado en que se deben incluir las cabeceras. Tengamos en cuenta que pueden aparecer dos cabeceras de opciones de destino. La primera se situaría antes de la cabecera de Encaminamiento y debería aplicarse a todos los saltos de la lista de la cabecera de Encaminamiento. La segunda debería de aparecer como última cabecera y se aplicaría sólo al destino final.

Es posible que algún día exista algún uso en que se envíe un paquete que conste de una cabecera sin carga útil. En este caso, el último campo Siguiente cabecera será 59, que significa «no sigue nada».

2.7.6.1. Uso de la cabecera de encaminamiento

La cabecera de encaminamiento es una función muy importante de la versión 6. Cuando se combina con las direcciones de envío a uno, puede usarse para controlar las rutas de acuerdo con las preferencias del proveedor o por la necesidad de usar un proveedor concreto, por ejemplo, para llegar a un usuario móvil. Recordemos que una dirección de envío uno se puede usar para decir «Vete por el encaminador más cercano que pertenezca al proveedor de servicios X».

Cuando se usa la cabecera de encaminamiento, el destino debe dirigirse de vuelta por esa ruta e invertir el camino hasta el origen.

2.7.6.2. Funcionamiento de la cabecera de encaminamiento

La cabecera de encaminamiento tiene un campo de tipo, que permitirá añadir distintos tipos en el futuro. En la actualidad sólo está definido el tipo 0. Una cabecera de encaminamiento de tipo 0 es similar a una ruta de origen de IPv4.

En la siguiente figura se muestra el formato de una cabecera de encaminamiento de tipo 0. La cabecera contiene una lista de nodos que hay que atravesar para llegar hasta el destino.

8 bits	8 bits	8 bits	8 bits
Cabecera siguiente	Tamaño de la parte de dirección	Tipo de encamina-miento = 0	Segmentos pendientes
8 bits	8 bits	8 bits	8 bits
Reservado	Máscara de bits estricta/relajada		
Dirección 1			
Dirección 2			
.....			
Dirección n			

Al igual que en la versión 4 el destino final es la Dirección n. El paquete se envía en primer lugar a la dirección de la cabecera principal de IPv6. A continuación se consulta la cabecera de encaminamiento. Se traslada la Dirección 1 al campo de dirección de destino de la cabecera de IPv6, se decrementa en uno el contador Segmentos restantes y se reenvía el paquete. La dirección final de la cabecera de encaminamiento es el destino real. Al llegar, la lista de direcciones contiene las direcciones de todos los nodos visitados.

La máscara de bits estricta/relajada indica si el salto correspondiente debe ser un vecino (estricta) o no (relajada).

2.7.6.3. Extensión de cabecera salto a salto

La cabecera salto a salto lleva información de opción que hay que examinar en todos los saltos de la ruta. En la siguiente tabla se muestra el formato de esta cabecera

8 bits	8 bits	16 bits
Cabecera siguiente	Tamaño de las extensiones de cabecera	
Opciones (tamaño variable)		

La cabecera salto a salto puede llevar un número variable de opciones. Cada una de ellas es autocontenida y se codifica en tres campos:

Tipo de opción	Tamaño de la opción	Valor de la opción
8 bits	8 bits	n bits

La opción carga útil extra es un ejemplo de opción de salto a salto. Se usa para declarar el tamaño de una carga útil de más de 64 Kilobits. El tamaño de la carga útil, en octetos, se describe por un valor de 4 bytes. El tamaño de la carga útil indicado incluye todo el paquete excepto la cabecera de IPv6.

2.7.6.4. Fragmentación

Al contrario que en la versión 4, la fragmentación **no la realizan nunca los encaminadores** sino sólo el nodo de origen. Se debería evitar la fragmentación siempre que fuese posible, pero a veces es necesaria. Es responsabilidad del nodo de origen el fragmentar los paquetes y el nodo de destino debe reensamblarlos.

Si un encaminador recibe un paquete demasiado grande para enviarlo, debe descartar el paquete y enviar de vuelta un mensaje de ICMP que indique la Unidad máxima de transmisión (MTU) del siguiente salto.ando un nodo de origen crea un fragmento, tiene que incluir una cabecera de Fragmento. En la siguiente figura se muestra el formato de la cabecera de fragmento.

8 bits	8 bits	13 bits	2	1
Cabecera siguiente	Reservado	Desplazamiento del segmento	Res	+
Identificación				

Como en la versión 4, el campo Desplazamiento de fragmento tiene 13 bits e indica desplazamientos en bloques de 8 octetos. El bit + indica si éste es el último fragmento o no. El campo Identificación se ha extendido hasta los 32 bits.

2.7.6.5. Opciones de destino

La cabecera de Opciones de destino contiene opciones que deben procesarse en el destino del paquete o en los destinos en el caso de multienvío. Actualmente, no se han definido opciones, distintas de los campos de relleno. En la siguiente figura se muestra el formato de esta cabecera.

8 bits	8 bits	16 bits
Cabecera siguiente	Tamaño	
Opciones (tamaño variable)		

Recordemos que si se incluye una cabecera de encaminamiento, el protocolo permite que se incluyan cabeceras de Opciones de destino. La primera, justo antes de la cabecera de encaminamiento contiene las opciones que aplican a todos los nodos de la lista de la cabecera. La segunda, situada tras el resto de las cabeceras, se aplica sólo al destino final.

2.7.7. Autoconfiguración de la versión 6

En el pasado, los administradores de redes hubiesen deseado disponer de una red de IP con pequeña carga de configuración y mantenimiento. Uno de los objetivos de la versión 6 es proporcionar un procedimiento efectivo de inicialización automática. Es importante para ayudar a que un lugar migre al

nuevo formato de direcciones. También es vital automatizar el cambio de direcciones que puede sobrevenir tras un cambio en la elección de proveedor de servicios.

En una LAN independiente, un host IPv6 puede construir automáticamente una dirección de IP usando una dirección de tarjeta interfaz de red u otro identificador único del nivel de enlace que conozca el sistema.

Cuando una organización tiene una red con un encaminador o está conectada a un proveedor de servicios, los encaminadores proporcionan a los host la información que debieran conocer para autoconfigurar sus direcciones y empezar a trabajar.

2.7.7.1. Función de los encamidares

Los encaminadores envían a los host información como:

- La dirección del encaminador.
- Una lista de todos los prefijos de direcciones que se usan en el enlace.
- Qué prefijos de host debería utilizar para crear su propia dirección.
- Una sugerencia sobre el límite máximo de saltos que debería usar.
- Información sobre si el host debe recuperar datos adicionales de configuración de un servidor del proveedor de configuración dinámica de host (DHCP - Dynamic Host Configuration Protocol).
- El valor de MTU para un enlace con MTU variable.
- Los valores de diversos temporizadores.

2.7.7.2. Lista de prefijos de direcciones

En IPv6 desaparecela necesidad de utilizar la máscara de subred. Las decisiones de encaminamiento se hacen comparando prefijos de direcciones.

Un encaminador anuncia la lista de prefijos de direcciones que se usan en el enlace local. El prefijo se expresa como parte de una dirección de IPv6, o toda junto con un número que indica cuántos bits pertenecen realmente al prefijo. Los host almacenan estas listas de prefijos.

Cuando un host necesita decidir si un destino está en el enlace o no, recorre la lista de los prefijos del enlace y compara el número de bits relevantes con los bits de la dirección de destino.

2.7.7.3 Direcciones de interfaz de IPV6

Todas las interfaces de la versión 6 tienen asociada una lista de direcciones. Como mínimo. la lista incluye la dirección local del enlace de la forma:

111111010 (10 bits)	00...00	Dirección única para la tecnología del enlace

Los nodos necesitan un mecanismo para generar su dirección única de interfaz de enlace. Por ejemplo en una interfaz de LAN la dirección de MAC es la única parte de una dirección que ocupa los 48 bits de más a la derecha Un sistema se puede comunicar con otro sistema del enlace usando su dirección local de enlace.

¿Cómo puede generar un host automáticamente direcciones locales al lugar o globales? Recordemos que un encaminador anuncia una lista de prefijos. Algunos de estos están marcados para construir direcciones de host. Una dirección local al lugar o global se construye situando un prefijo de esos al inicio de una dirección única de enlace. Esta dirección se añade a la lista de host.

El anuncio del encaminador también indica si deberían recoger información adicional de dirección de un servidor de DHCP quien puede asignar direcciones configuradas por el administrador. Y el anuncio indica si esta información adicional de configuración debería obtenerla de un servidor.
Asimismo, si alguien quiere utilizarla también se puede usar configuración manual en la versión 6.

2.7.7.4 Cambio de direcciones

La posibilidad de usar más de un prefijo global facilita la transmisión de un proveedor de servicios a otro.

Los anuncios del encaminador asocian a cada prefijo de proveedor un temporizador de caducidad. Cuando se cambia de un proveedor a otro, se deja que el antiguo prefijo caduque. Por supuesto, los valores de caducidad de un prefijo nuevo, activo, se reactivan periódicamente para que no caduquen.

Estos plazos también permiten llevar un host y conectarlo a un enlace diferente del lugar. Dado que el prefijo incluye el identificador de subred así como el proveedor y la información regional. Los antiguos prefijos irán caducando y se irán aprendiendo los nuevos.

2.7.7.5. Comprobación de que las direcciones son únicas

Antes de usar la dirección local del enlace, el host debe multienviar una solicitud que compruebe si la dirección ya se está usando en el enlace. De esta forma se asegura que la dirección de IP local del enlace. y todas las direcciones que se formen con ella con un prefijo diferente. son únicas. Las direcciones que se configuran manualmente, o que se aprenden de un servidor de DHCP, también se comprueban antes de usarse.

2.7.8. Configuración mediante DHCPv6

Los sistemas pueden obtener un conjunto completo de parámetros de configuración de un servidor de DHCP. Para migrar a la versión 6 de DHCP hay que hacer algunos cambios.

Obviamente, el nuevo protocolo debe permitir las direcciones de la versión 6. Además. el antiguo temporizador de alquiler se sustituye por los tiempos de vida de depreciación e invalidación.

Se pretende que DHCPv6 no sólo autoconfigure host sino también registre automáticamente nombres y direcciones de host en el Sistema de nombres de dominio.

Un host, en su inicialización, puede solicitar el uso de un nombre de host concreto o le puede asignar un nombre el servidor de DRCPv6.

Si expira el tiempo de vida de invalidación del cliente, el servidor de DHCPv6 debería de eliminar el registro de DNS del cliente.

2.7.9. Transición a IPv6

Dada la universalidad de utilización de IP, está claro que la transición debe ser gradual.

- Los nodos de la versión 6 necesitan interconectarse con nodos de versión 4.
- No se puede forzar a las organizaciones a abandonar sus direcciones actuales.
- Las organizaciones deberían ser capaces de actualizar algunos nodos. dejando otros sin cambiar.

- La transición debería ser fácil de entender y realizar. Dada la universalidad de utilización de IP, está claro que la transición debe ser gradual.
- Los nodos de la versión 6 necesitan interconectarse con nodos de versión 4.
- No se puede forzar a las organizaciones a abandonar sus direcciones actuales.
- Las organizaciones deberían ser capaces de actualizar algunos nodos. dejando otros sin cambiar.
- La transición debería ser fácil de entender y realizar.

2.7.9.1. Como realizar el cambio

El primer paso para cambiar a la versión 6 es actualizar el software del Servidor de nombres de dominio de manera que el DSN responda a las solicitudes que usan el nuevo formato de direcciones.

Es muy probable que los primeros sistemas que se conviertan con versiones duales de los protocolos sean los encaminadores que hacen de interfaz con las redes externas. Poco a poco. los servidores importantes añadirán una pila de la versión 6. En un entorno mezclado, el tráfico de la versión 6 tendrá, a veces, que ser encapsulado a través de redes con la versión 4

En el período de tiempo de este proceso, se pueden usar las direcciones locales del lugar de IPv6. Cuando los lugares se conecten a un proveedor de servicios, las direcciones crecen con los prefijos apropiados de región, proveedor y cliente.

2.7.9.2. Cambios en el DNS

Existe un nuevo tipo de registro de recurso dirección, AAAA, que hace corresponder nombres de dominio a direcciones de la versión 6 de IP. Una entrada de ejemplo es:

MICKEY IN AAAA 4321:0:1 :2:3:4:567:89AB

También tiene que disponer de búsquedas inversas. Se ha añadido un nuevo dominio para manejar la asociación de dirección a nombre de IPv6. El dominio de búsqueda inversa tiene su raíz en IP6.INT.

Recuerde que las direcciones de IP de la versión 4 se invierten para obtener sus etiquetas en el dominio in-addr.arpa. Una dirección de la versión 6 también se invierte y se rescribe con una serie de dígitos hexadecimales separados por dos puntos. Por ejemplo, una entrada de búsqueda inversa para:

4321:0:1:2:3:4:567:89AB

aparece en el árbol de dominios como:

B.A.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0. 1.0.0.0.0.0.0.0.1 .2.3.4.IP6.INT

2.7.9.3. Encapsulamiento a través de una red con la versión 4

Durante el período de transición, los datagramas deberán atravesar a veces un camino como el que se muestra en la siguiente figura.

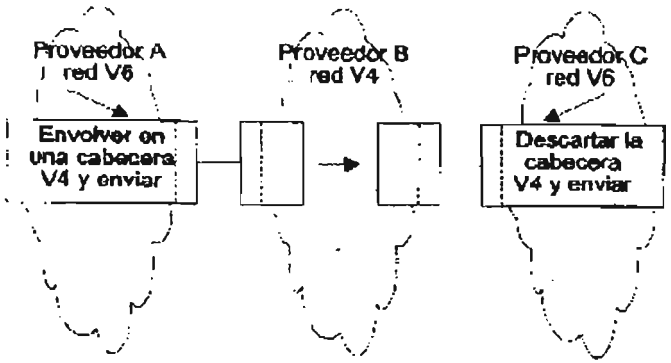


Fig. 59. Encapsulamiento de tráfico a través de una red de la versión 4.

Figura 2.46 Encapsulamiento de tráfico a través de una red de la versión 4

En la figura, los proveedores de servicios A y C disponen de la versión 6, pero el proveedor de servicios B no. A las interfaces del encaminador de frontera se le asignarán direcciones de IPv6 compatibles con IPv4, que se pueden convertir fácilmente a direcciones de la versión 4 eliminando sus prefijos a cero. Los paquetes de la versión 6 se empaquetarán dentro de cabeceras de la versión 4 y se encapsulan a través de las redes implicadas.
También puede ocurrir el encapsulamiento cuando un lugar ha convertido algunas de sus redes a la versión 6. Se puede usar el encapsulamiento siempre que sea conveniente hacerlo. Se puede usar entre encaminadores. entre host o en un camino host-encaminador.

CAPITULO 3. Protocolos de control de acceso al medio y Estándares de Redes

3.1. INTRODUCCIÓN

La definición que siempre me ha gustado más sobre lo que es una red de área local es la dada por el IEEE (Institute of Electrical and Electronics Engineers); **"Una red de área local es un sistema de comunicación de datos que permite a un cierto número dispositivos independientes comunicarse directamente entre sí, dentro de una área geográfica reducida y empleando canales físicos de comunicación de velocidad moderada o alta".**

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas ofimáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más difundida, la Ethernet, utiliza un mecanismo denominado Call Sense Multiple Access-Collision Detect (CSMS-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos a 10 Mbits/seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay topologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.
Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales.

3.2 Protocolos de control de Acceso al medio.

Todas las redes locales consisten en una colección de dispositivos que deben compartir la capacidad de transmisión de la red. Por esta razón es necesario tener un control de acceso al medio de transmisión para que dos dispositivos particulares puedan intercambiar datos cuando sea requerido dentro de un esquema centralizado o distribuido.

En un esquema centralizado, se designa un controlador con la suficiente autoridad para garantizar el acceso a la red. De esta manera, una estación que desee transmitir deberá esperar a recibir el permiso del controlador. Se suele utilizar en topologías lógicas de bus. En una red descentralizada (distribuida) o pasa de testigo, las estaciones colectivas desarrollan una función de control de acceso al medio, materializada en una trama especial denominada "token" (testigo) que va pasando de estación en estación, para determinar dinámicamente el orden en el cual transmitirán las estaciones. Una estación para transmitir debe poseer el "token", cuando se acaba la transmisión se pone otra vez en circulación el "token".

En general se pueden clasificar a las técnicas de control de acceso en síncronas y asíncronas.

3.2.1. Técnicas Síncronas

Con las técnicas síncronas, una capacidad específica es dedicada para realizar una conexión (se utiliza en redes locales de circuito conmutados, cabe mencionar que no son muy óptimos para redes LAN y WAN por que las necesidades de transmisión de las estaciones se puede decir que son impredecibles).

3.2.2. Técnicas Asíncronas

Otra forma de realizar una conexión más eficazmente para redes locales, serían las técnicas asíncronas. Las cuales se pueden subdividir en tres categorías: round robin, reservación y contención.

	Topología en Bus	**Topología en Anillo**
Round Robin	Token buns (IEEE 802.4)	Token Ring (IEEE 802.5,FDDI)
Reservación	MAN (IEEE 802.6[1])	
Contención	CSMA/CD (IEEE 802.3)	

Nota: todos los protocolos MAC son protocolos distribuidos, con excepción de IEEE802.6 y FDDI-II que son protocolos para tráfico de circuitos conmutados y pueden ser distribuidos o centralizados.

Round Robin

Esta técnica es basada en darle a cada quien un turno para trasmitir, durante este turno la estación puede declinar la transmisión o puede transmitir sujeto a un cierto limite. El control en esta técnica puede ser de modo distribuido o centralizado. Este tipo de control de acceso al medio es utilizado en las topologías en bus mediante token bus, y en las topologías anillo mediante token ring.

Token Bus (Paso de testigo en bus)

En este caso se define un anillo lógico, es decir en bus, pero la topología lógica es en anillo. Las estaciones se organizan para saber de quién tiene que recibir el testigo y a quien se lo deben de enviar. Con este método de control se pueden implementar esquemas de transmisión deterministicos y con prioridades, fundamentales en algunas aplicaciones de monitorización y control de procesos industriales. Se utiliza sobre topología física.

Token Ring (Paso de testigo en anillo)

El testigo va pasando de estación a estación en una red con tipología en anillo. La estación que desea transmitir espera la llegada del testigo, lo captura y comienza la transmisión. A su vez retira del anillo sus datos una vez que han circulado por el mismo. Al finalizar retransmite el testigo. En recepción la estación copia los datos que pasan por ella y cambia algunos bits de redundancia con el fin de señalizar al transmisor la recepción de los mismos.

Uno de los inconvenientes de este método es que, al llegar el token a la estación, regenera el mensaje antes de pasarlo a la siguiente estación. Esto origina una reducción en el rendimiento de la red, pero se asegura una transmisión exitosa. Desde la primera vez que se envía el mensaje.

Reservación

En está técnica, el tiempo sobre el medio de transmisión es dividido dentro de ranuras (frames). Una estación que desea retransmitir, reserva ranuras futuras para un periodo indefinido. La reservación de las ranuras puede llevarse a cabo de una manera distribuida o centralizada.

Contención

En está técnica todas las estaciones que desean transmitir información compiten por la utilización del medio transmisión y en caso de que varias a la vez

transmitan, provoca que la información se pierda en el canal por colisión de las señales procedentes de múltiples estaciones. Esta señal de colisión suele consistir en una sobre tensión de línea, para la cual los dispositivos de transmisión han de estar preparados para no resultar dañados.

Este tipo de técnicas se utiliza cuando varias estaciones pueden tener acceso a la ves al mismo medio de transmisión. Este es el caso de la topología física en bus con lógica también en bus. A los canales de difusión se les conoce como "canales de acceso aleatorio" o "canales multiacceso" y se conocen muchos protocolos para solucionar el problema de las posibles colisiones. A continuación, se describen los métodos más utilizados.

Protocolos sin escucha

Son protocolos que no comprueban si el medio está siendo utilizado. Cuando una estación desea transmitir, pone o inserta directamente los mensajes en el canal, existiendo un tamaño máximo de información que se puede enviar. Si al cabo de mucho tiempo no ha recibido respuesta, supone que se ha producido una colisión y reenvía los datos. La idea original de estos protocolos procede del sistema ALOHA, diseñada por Norman Abramsom y sus colaboradores, en 1970, para interconectar por radio las computadores y terminales de las universidades de las islas Hawai. Si se hace un cálculo de la eficiencia de este sistema se obtiene que es del orden del 18%. Se han introducido mejoras a este esquema básico, por ejemplo la técnica denominada ALOHA_ranurado, que incorpora una referencia de tiempo para que las estaciones solamente puedan transmitir en los instantes predeterminados por la señal de reloj. Está técnica disminuye la probabilidad de colisiones.

Protocolo con escucha

Estos protocolos, denominados en inglés CSMA (Carrier Sense Multiple Access) pertenecen a las dos capas más bajas del modelo OSI, capa física y capa de enlace de datos y definen cómo múltiples computadoras pueden usar simultáneamente la red sin interferir unas con otras.

El proyecto IEEE 802, del que se hablará posteriormente, trabaja con las especificaciones de estas dos capas. El estándar 802 define con más detalle la capa de enlace de datos, para lo cual se divide en dos subcapas:

- Logical Link Control (LLC) Control de enlace lógico
- Media Access Control (MAC) Control de Acceso al medio

❖ Subcapa LLC

Esta subcapa define el protocolo que asegura que los datos se transmitan de forma fiable a través del enlace de comunicaciones. El LLC suministra los siguientes servicios:

- Servicio orientado a conexión en el cual se estable una sesión con destino y se libera cuando se completa la transferencia de datos.
- Servicio sin conexión, en el cual no se establece una conexión ni se confirma su recepción.

❖ Subcapa MAC

La subcapa de control de acceso al medio (Media Access Control) es la mas baja de las dos subcapas (esta más cerca de la Capa Física), provee de acceso compartido a la capa física para todas las interfaces de red de las estaciones. La subcapa MAC se comunica directamente con la interfaz de red y es responsable de una comunicación libre de error entre dos estaciones en la red.

A estos protocolos se les denominan con escucha porque las estaciones pueden detectar si está libre o no el medio de transmisión e incluso pueden escuchar su propia señal después de la transmisión, para impedir o detectar colisiones. Así, si una estación desea transmitir, escucha el canal, y si esta libre, envía los datos.

Este protocolo no garantiza que no se produzcan colisiones. Si t es el tiempo que tarda una trama en llegar al punto más alejado del origen, entonces el período vulnerable es 2t. si suponemos que una estación situada en un extremo de la red desea transmitir y encuentra el canal libre. Entonces empieza a enviar información. Si justo antes de que la trama llegue a la última estación en tiempo t, ésta se pone a transmitir, se producirá una colisión, que tardará un tiempo adicional t en alcanzar a la estación original. Así, la primera estación deberá escuchar el canal durante t + t = 2t. transcurrido este tiempo, se garantiza que no se producirán colisiones.

A continuación se comentarán algunas modalidades de protocolos con escucha:

CSMA 1-persistente

Las estaciones antes de transmitir escuchan el canal y solamente si detectan que está libre, transmiten su trama.

En cada caso de que el canal esté ocupado esperan escuchando hasta que quede libre. De aquí el nombre de 1-persistente, porque la estación transmite con probabilidad 1, es decir, siempre que una estación desee transmitir, logrará hacerlo, pero es posible que no se haga con éxito, pues puede producirse una

colisión. Si ocurriera una colisión la estación espera un tiempo aleatorio[1] y comienza de nuevo.

Este tipo de protocolos consigue una baja tasa de colisiones si hay pocas estaciones que deseen transmitir a la vez (baja carga). No es adecuado para redes con carga elevada, pues ocurrirá muchas veces que haya dos estaciones esperando a que el canal quede libre. En cuanto ocurra esto, enviarán sus datos simultáneamente, produciéndose inmediatamente después una colisión.

CSMA no persistente

Las estaciones antes de transmitir escuchan el canal y solamente si detectan que está libre transmiten su trama, como el caso anterior. En caso de que el canal, esté ocupado no siguen escuchando el canal sino que espera un tiempo aleatorio y comienza de nuevo.

De esta forma se pierde algo de tiempo cuando hay baja carga, pero reduce el número de colisiones cuando hay muchas estaciones deseando transmitir (alta baja). Visto de otra forma, cuando sólo una estación desea transmitir y encuentra el canal ocupado, tendrá que esperar un tiempo aleatorio, en principio mayor que el estrictamente necesario para que el canal quede libre. Así, se estará perdiendo tiempo. Sin embargo, si varias estaciones desean transmitir y encuentran el canal ocupado, esperarán un tiempo aleatorio (distintos entre sí), de forma que se evitará la colisión segura del protocolo 1-persistente.

CSMA p-persistente

Este protocolo se aplica a canales rasurados en los que hay una referencia de tiempo que comparten todas las estaciones, de tal forma que cada estación solamente puede comenzar la transmisión de la trama en instantes predeterminados. Cuando una estación detecta que el canal está libre aplica la siguiente regla: transmite con una probabilidad p y espera la siguiente ranura con una probabilidad de q=1-p. El proceso se repite hasta que la estación ha transmitido la trama u otra estación ha comenzado a transmitir, en cuyo caso se actúa como si hubiera sucedido una colisión. Se espera un tiempo aleatorio y se comienza de nuevo.

[1] La aleatoriedad del tiempo se incrementa de forma binaria exponencial. A este proceso de detenerse y volver a intentar se le llama Backoff. El Backoff es realizado 6 veces y si no se logra transmitir el paquete, el envió se descarta. Por esto en Ethernet puede existir pérdida de paquetes.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

Aquí, la variación respecto al CSMA es que las estaciones abordan la transmisión tan pronto como detectan una colisión. Con un sistema CSMA/CD, se supone que las colisiones son una incidencia operacional normal. El CSMA/CD esta basado en el concepto: "escuchar antes de hablar" (listen before talking). Significa que antes de que la estación transmita, toma un momento para verificar que nadie más está usando (escuchando) el canal de comunicación. De otra manera, espera un tiempo y vuelve a revisar si la red esta libre. El método no es el más seguro, ya que si dos estaciones "escuchan" y transmiten al mismo tiempo, los mensajes chocaran (existe una colisión) y los datos se perderán. Para compensar esta dificultad, las estaciones volverán a transmitir si descubren que los datos no se recibieron de forma correcta. En los protocolos anteriores, si se empieza a transmitir no se para, aunque se produzca colisión, ya que ésta no es detectada. Cuando para un tiempo si recibir respuesta, considera que se ha producido colisión, transmiten una señal especial denominada <<jamming>> para asegurar que las demás estaciones detectan también la colisión.

Para garantizar que se detectan la colisión durante la transmisión de la trama, se debe cumplir que el tiempo de transmisión de la trama tt ha de ser mayor que el máximo retardo de la señal por el medio de transmisión (el tiempo de propagación entre las estaciones más alejadas de la red), es decir, tt>=2 td. Luego siempre que se aplique este protocolo hay que tener en cuenta este compromiso entre longitud de la trama y longitud de la trama y longitud del medio de transmisión.

CSMA/CA (Carrier Multiple Access/Collision Avoidance)

Aquí la variación respecto al caso anterior es que se trata de evitar colisiones avisando, mediante la transmisión de una trama corta (ráfaga de portadora), a las demás estaciones que se va a transmitir. Cualquier estación al escuchar esta ráfaga no debe intentar transmitir hasta después de que suceda la transmisión de la correspondiente trama anunciada por la ráfaga. A pesar de todo, se pueden producir colisiones al enviar la ráfaga de portadora (cuando varias estaciones desean transmitir a la vez e intentan avisar a las demás).

3.3. Estándares de Redes

3.3.1. Estándares de IEEE

El IEEE (Institute of Electrical and Electronics Engineers) desarrolló una serie de estándares conocidos como IEEE 802.x para redes de área local. Estos estándares fueron adoptados por ISO.

El estándar IEEE 802.x está integrado por varios subcomités que están organizados de la siguiente manera:

802.1 Interfaces de redes de alto nivel y puentes MAC (HLI, High Level Interface)
802.2 Control de enlace lógico (LLC, Logical Link Control)
802.3 Acceso, múltiple con detección de portadora y detección de colisiones (CSMA/CD, Carrier Sense Multiple Access with Collisión Detect)
802.4 Token Bus
802.5 Token Ring
802.6 Redes de área metropolitana (MAN, Metropolitan Area Networks)
802.7 Grupo asesor para técnicas de banda ancha (Broadband Technical Advisory Group)
802.8 Grupo asesor para técnicas de fibra óptica (Fiber Optic Technical Advisor Group)
802.9 Redes integradas por voz y video (integrated Data and Voice Networks)
802.10 Seguridad de red (LAN Security)
802.11 LAN de acceso de prioridad por demanda (100VG Anylan)
802.12 Redes inalámbricas de área personal (Gíreles Personal Area Netwoks)
802.14 Cable de T.V.
802.15 Redes inalámbricas de área personal (Gíreles Area Netwoks)

Estos estándares cubren la capa física y la capa de enlace de datos de modelo de referencia OSI.

3.3.2. IEEE 802.1 Interfaces de redes de alto nivel y puentes MAC

El estándar 802.1 es una introducción del grupo de estándares 802.x de redes de área local y define las primitivas de la interfaz, en las que se incluyen: el sistema de direcciones, administración de las redes y puentes.

Sistema de direcciones de IEEE 802

Una red local al ser multipunto hace que cada estación conectada en la red examine cada paquete que se transmite en esta por lo que es necesario que cada paquete que se transmita contenga un campo con la dirección de la estación destino y otro campo con la dirección de la estación fuente.

El subcomité 802.1 hizo la estandarización del sistema de direcciones para redes locales en el que se estableció una longitud de 48 bits (el rango de una dirección entera, 6 octetos) para cada dirección, que es suficiente como un identificador global único para cada dispositivo de red. Basándose en lo anterior, cada dispositivo de red tiene una dirección física única que es asignada por el fabricante en el momento de su fabricación. Esta dirección además de conocerse como

dirección física también se le conoce como dirección de hardware o dirección MAC (Media Access Control).

Actualmente la organización IEEE se encarga de la administración universal para la asignación y manejo de rango de direcciones. Cuando un fabricante desea fabricar equipo que se comunicará en red primero debe hacer una petición para obtener un bloque de direcciones, cada bloque consta de 2^{24} direcciones, o sea 24 bits. Al fabricante se le asignan tres octetos de valor fijo (24 bits), este bloque de valor fijo de direcciones es referido también dentro de la industria como código del vendedor u OUI (Organizationally Unique Identifier). Los tres octetos restantes (24 bits) son asignados por el fabricante para cada uno de sus productos.

En la actualidad los 24 bits de valor fijo (OUI) tienen una estructura adicional que consta de dos bits de control. El primer bit de control representa un grupo/individual. Si el bit es cero la dirección se refiere a una estación particular o individual, o bien si el bit es 1, la dirección es referida a un grupo lógico de estaciones que necesita mayor resolución.

El segundo bit es el bit universal/local. Si el bit es 0, quiere decir que la dirección fue establecida por la autoridad administrativa universal (significa que los siguientes 22 bits fueron asignados por el IEEE). Si el segundo bit tiene valor de 1, el campo OUI fue asignado en forma local. Como conclusión, la autoridad global asigna 22 bits de valor fijo, un bit para indicar grupo/individual y un bit para indicar universal/local. En la siguiente figura se muestra el direccionamiento del IEEE 802.

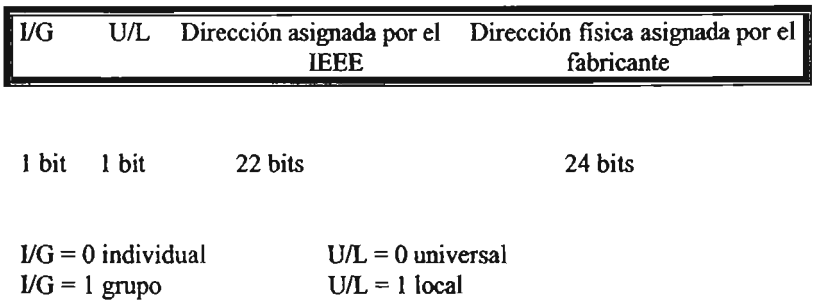


Figura 3.1Esquema de direccionamiento del IEEE 802

En el caso en que un fabricante se quedara sin direcciones físicas, el IEEE tiene la capacidad de asignarle un segundo identificador OUI.

Direcciones multicast y broadcast

Una dirección multicast permite que un solo paquete sea recibido por un grupo seleccionado de estaciones. El programa de red puede establecer que la configuración de la interfaz de red de una estación escuche una dirección específica de multicast. Esto hace posible que un conjunto de estaciones sean asignadas a un grupo multicast el cual se le ha asignado una dirección multicast específica. Un solo paquete enviado a la dirección multicast asignada a este grupo será recibido por todas las estaciones en dicho grupo.

Hay otro caso de dirección multicast llamado broadcast o de difusión. En esta dirección los 48 bits son establecidos en el valor 1. Todas las interfaces Ethernet que verifican un paquete con esta dirección destino, lo leerán y lo entregarán al programa de la capa de red de la estación.

IEEE 802.1A
Este subcomité se encarga de proveer una arquitectura con manejo en red consistente con el modelo OSI.

IEEE 802.1B
Este subcomité desarrolla protocolos de manejo y administración de reces del tipo LAN Y MAN (Metropolitan Area Networks). Estos estándares tienen como objetivo ser complementos para los estándares de administración de sistemas referidos en OSI, tales como SNMP (Simple Network Management Protocol) y CMIP (Common Management Information Protocol).

IEEE 802.1D
En este subcomité se define el estándar para el encaminamiento por medio de puentes (bridges) bajo consideración del IEEE. Este encaminamiento es distribuido sobre múltiples redes LAN conectadas a través de estos dispositivos. Este estándar ha adoptado el algoritmo de enrutamiento "Spanning tree" que se utiliza en puentes para redes locales de tipo Ethernet.

IEEE 802.1G
El subcomité 802.1G ha trabajado en el desarrollo de un estándar para el encaminamiento de puentes remotos (remote bridges) en redes de área amplia WANs (Wide Area Networks). Se adoptó el algoritmo de encaminamiento "Spanning tree" que es utilizado en redes de área local como se mencionó en el estándar 802.1D.

3.3.3. IEEE y la capa de enlace de datos del modelo OSI

Los protocolos que operan al nivel de la capa de enlace de datos del modelo de referencia OSI, se encargan de que la transmisión de las tramas de información sea eficaz y sin errores entre dos estaciones adyacentes, es decir, entre estaciones sin nodos de conmutación intermedios. Las funciones de la capa de enlace consisten en el control de flujo de datos entre un nodo emisor y un nodo receptor realizando una sincronización lógica en su comunicación además de controlar y detectar errores en la secuencia de los paquetes de datos obtenidos por el nodo receptor.

El estándar IEEE divide el nivel de la capa de enlace de datos en dos subcapas: la capa Control de Acceso al Medio MAC (subcomité 802.3,802.4 y 802.12) y la capa nivel Control Lógico de Enlace LLC (subcomité 802.2)[3].

Las funciones asociadas en el nivel de enlace de datos para realizar la transmisión y recepción entre estaciones conectadas a una red local son:

- Proveer uno o más puntos de acceso a servicio SAP (Service Access Point) para soportar la característica de multiacceso del enlace.
- Realizar ciertas funciones que le corresponden a la capa 3 del modelo OSI referido como la capa de red.
- En la transmisión, lleva a cabo el ensamblado de datos dentro de un paquete con los campos correspondientes a las direcciones[4] y el método CRC para detección de errores.
- En la recepción, lleva a cabo él desensamble del paquete, desarrollando el reconocimiento de las direcciones y la validación con el método de detección de errores CRC.
- Debe administrar el acceso al medio compartido de las redes locales para llevar a cabo la transmisión.

Las dos primeras funciones son desarrolladas por la subcapa LLC, las últimas tres son desarrolladas por la subcapa de control de acceso al medio MAC. Esta subdivisión en la capa de nivel de enlace tiene dos razones:

Se satisface la lógica requerida para administrar el acceso al medio compartido para redes multipunto, las cuales no se contemplan en el nivel de enlace de datos tradicional. La subcapa LLC sirve como interfaz para los protocolos de las capas

[3] Estas subcapas que se establecen dentro de la capa de enlace no se toman en consideración en el tradicional modelo de referencia OSI.

[4] Los campos de direcciones fuente y destino se llevan a cabo en la subcapa MAC de la capa de enlace. De esta manera cada subcomité (802.3,802.4 y 802.5) puede definir sus direcciones de manera independiente a la subcapa LLC.

superiores (principalmente la capa de red) logrando con esto aislar niveles superiores de las acciones especificas llevadas a cabo por la subcapa MAC, como es el control de acceso al medio. De esta forma se tiene el uso de una misma subcapa LLC para varias operaciones a escoger de la subcapa MAC (802.3,802.4 y 802.5 Y 802.12) logrando así una mayor flexibilidad de los niveles inferiores del modelo OSI y además de poder soportar diversas opciones de pilas de protocolos en las capas superiores. Dentro de los estándares definidos por el IEEE también se han definido las características para el nivel físico como son:

- Tipo de medio para las respectivas topologías que soportan las diferentes opciones de subcapa de MAC[5].
- Transmisión y recepción de bits
- Codificación y decodificación de señales
- Preámbulo de generación y remoción (para la sincronización), etc.

En la siguiente figura se muestran los protocolos IEEE para redes LAN en las capas interiores del modelo de referencia OSI.

SAP						Subcapa LLC
802.2 tipo 1, tipo 2 y tipo 3						
MSAP	**MSAP**	**MSAP**	**MSAP**	**MSAP**	**MSAP**	
802.3 CSMA/CD Ethernet y Fast Ethernet	802.4 Token Bus	802.5 Token Ring	802.6 Redes de Area Metropolitana (MAN)	802.9 Redes Integrales (IVD) Voz/Datos	802.12 100VG AnyLAN	Subcapa MAC **Capa de enlace de datos**
PSAP	**PSAP**	**PSAP**	**PSAP**	**PSAP**	**PSAP**	**Capa Física**
PHY	PHY	PHY	PHY	PHY	PHY	

LLC: Control de Enlace Lógico
MAC: Control de Acceso al Medio
LSAP: LLC Punto de Acceso al Servicio
MSAP: MAC punto de Acceso al Servicio
PSAP: Punto de Acceso Físico

Tipo1 servicio sin conexión.
Tipo 2 Servicio orientado a conexión
Tipo3 servicio con conexión

Figura 3.2 Protocolos de redes LAN del IEEE.

[5] Es importante señalar que en el modelo de referencia OSI no se referencia de ningún tipo de medio físico.

En la figura anterior se pueden observar la división MAC – LLC en la capa de enlace, obteniendo con esto varias ventajas, como el controlar el acceso al canal compartido entre los dispositivos (Subcapa MAC) además de tener un esquema descentralizado que reduce la susceptibilidad de errores en la red. Por último, brinda una interfaz más compatible con las redes de área amplia (WAN), partiendo de la idea de que el LLC es un subconjunto del protocolo HDLC. LLC es independiente de un método de acceso al medio, mientras que la MAC es un protocolo específico dependiente del diseño. El resultado de esta división hace más fácil el diseño de las redes al proveer una interfaz con mayor flexibilidad para las redes locales.

3.3.4. IEEE 802.2 Control de Enlace Lógico (LLC, Logical Link Control)

El estándar 802.2 fue creado por el IEEE con el fin de desarrollar un protocolo de enlace de datos que lleve a cabo tareas de control de errores y control de flujo. Este protocolo puede operar encima de todos los protocolos LAN y MAN 802. Otra característica importante es que puede esconder las diferencias entre los distintos tipos de redes 802, de tal manera que puede proporcionar un formato único y una interfaz con la capa de red[6]. En la siguiente figura muestra el LLC como parte superior de la capa de enlace, con la subcapa MAC por debajo de él.

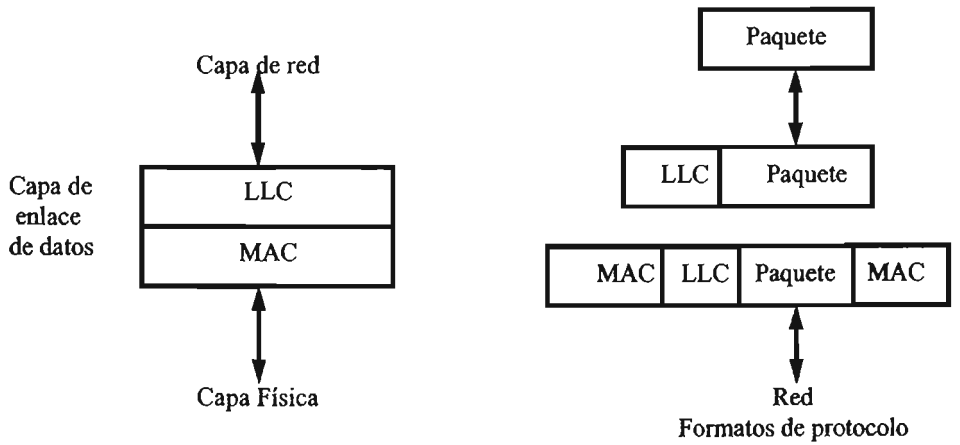


Figura 3.3 Posición del LLC

[6] Este formato, interfaz y protocolo están basados estrechamente en el modelo OSI.

Normalmente el protocolo LLC se utiliza de la siguiente manera: La capa de red de la estación que transmite datos pasa un paquete al LLC usando las interfases de acceso al LLC llamadas LSAPs[7] (Link Service Access Points). La subcapa LLC entonces agrega una cabecera LLC que contiene los números de secuencia y acuse. La estructura resultante se introduce entonces en el campo de carga útil de una trama 802.x y se transmite. En el receptor ocurre el proceso inverso.

El protocolo LLC proporciona tres opciones de servicio[8]: servicio sin conexión sin reconocimiento (Unacknowledge Connectionless Service), servicio sin conexión con reconocimiento (Acknowwledge Connectionless Service), y servicio confiable orientado a conexión.

- Servicio sin conexión sin reconocimiento. Este es un servicio de datagrama que únicamente permite el envío y recepción de paquetes LLC sin ninguna forma de reconocimiento (acknowledge) que asegure la entrega. Esto es debido a que cada paquete lleva la información completa de la dirección fuente y destino. No hay manera de garantizar que los paquetes llegaron intactos o en el orden adecuado. Este servicio soporta transmisiones punto a punto, multipunto y broadcast.
- Servicio sin conexión con reconocimiento. Este es un servicio sin conexión, pero con reconocimiento, es decir, se tiene un mecanismo por el cuál cada usuario puede enviar una unidad de datos y recibir un reconocimiento (acknowledgement) de que todos los datos fueron entregados sin la necesidad de establecer una conexión lógica. En estos procesos también se lleva a cabo la corrección de datos erróneos retransmitiendo los paquetes que contienen dichos datos, esto libera a los niveles superiores de esta tarea. Este servicio soporta transferencias punto a punto.
- Servicio orientado a conexión. Este servicio establece un estilo de conexión de circuito virtual entre LSAP's. Con esto provee una medida por la cuál un usuario puede hacer una petición o ser notificado del establecimiento o terminación de una conexión lógica. El servicio orientado a conexión también provee un control de flujo, funciones de secuencia, y control de errores. Este servicio incluye un conjunto de primitivas de petición, indicación, respuesta y confirmación para establecer una conexión lógica entre LSAP's, una vez que una conexión es establecida, los bloques de datos son intercambiados garantizando que todos estos serán entregados debido a la conexión lógica existente y no existe la necesidad de un reconocimiento (acknowledgement) de cada bloque de datos. El control de

[7] LSAP son direcciones de enlace de datos lógicos para puntos de acceso. Una sola dirección MAC puede tener múltiples direcciones LSAP. Estas múltiples direcciones habilitan múltiples conexiones punto-final (end-point) entre dos nodos de una red local.

[8] Esta especificación de los tres tipos de servicios fue el resultado de permitir al protocolo LLC ser utilizado para soportar los diversos requerimientos de los usuarios.

- flujo puede ser controlado en cualquier dirección. Este servicio soporta direccionamiento punto a punto.

Funciones de la capa de red realizados por el nivel de enlace de datos de redes LAN

Las redes de área local al ser multipunto, no cuentan con nodos de conmutación intermedia por lo que hace que no se requiera del nivel 3 del modelo de referencia OSI (capa de red) ya que las funciones esenciales de dicho nivel pueden ser incorporadas dentro del nivel 2 (capa de enlace), como son:

1. Servicio sin conexión (Connectionless). Este es un servicio que no requiere establecer una conexión lógica para optimizar el soporte de tráfico altamente interactivo.
2. Servicio orientado a conexión.
3. Servicio de Multiplexaje. Comúnmente, un solo enlace físico une una estación a la red local; esto deberá de ser posible para proveer transferencia de datos con múltiples puntos terminales/finales sobre el enlace.

Estas tres funciones mencionadas son llevadas a cabo por el nivel 2 del modelo OSI debido a que no se requiere llevar a cabo un enrutamiento en las redes locales.

El nivel 2 también lleva a cabo la tarea de multicast y broadcast. El nivel de enlace deberá proveer un servicio para enviar un mensaje a múltiples estaciones y de esta manera tomar ventajas de la naturaleza de acceso múltiple de una red local.

3.3.5. IEEE 802.3 Estandarización de la tecnología Ethernet CSMA/CD

El estándar IEEE 802.3 es para una red de área local con el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detect), cuando una estación quiere transmitir, escucha el cable. Si el cable está ocupado, la estación espera que se desocupa; de otra manera, transmite de inmediato. Si dos o más estaciones comienzan a transmitir simultáneamente por un cable inactivo, habrá una colisión. Todas las estaciones en colisión terminan entonces su transmisión, esperan un tiempo aleatorio y repiten una vez más el proceso.

La tecnología Ethernet[9] es también llamada red de bus CSMA/CD. El método de control de acceso al medio y el formato del paquete Ethernet es idéntico para

todas las variedades de velocidad en las que ellos operan y los medios soportados por Ethernet.

Cableado del 802.3 (Ethernet)

El nombre Ethernet[10] hace referencia al cable. Cada estación equipada con Ethernet, opera de forma independiente de todas las demás estaciones sobre la red, es decir, no existe un controlador central. Todas las estaciones unidas en un sistema Ethernet son conectadas a un sistema de señal compartido, también llamado bus o backbone. Las señales Ethernet son transmitidas de forma serial, un bit a la vez sobre el canal de de señal compartido, el cual es recibido por cada estación conectada al bus. El acceso al canal compartido es determinado por un método de control de acceso (MAC) llevado a cabo en cada interfaz Ethernet localizado en cada estación. Ethernet ocupa el mecanismo de control de acceso al medio llamado CSMA/CD. Comúnmente se utilizan cinco tipos de cableado, como lo muestra la siguiente tabla.

	10Base 5	10Base2	10BaseT	10BaseF
Medios de Transmisión	Coaxial grueso	Coaxial degado	Par trenzado (UDP)	Fibra óptica
Diámetro del cable (mm)	10	5	0.4-0.6 (22-26AWG)	
Tasa de transmisión de datos (Mbps)	10	10	10	10
Segmento máximo	500	200	100	2000
Técnica de señal utilizada	Baseband Manchester	Baseband Manchester	Baseband Manchester	Baseband Manchester
Nodos por segmento	100	30		1024
Ventajas	Bueno para backbone	Sistema económico		Mejor entre edificios

Tabla 3.2 Los tipos de medios más comunes en LANs 802.3

10Base 5

El cable 5 10Base5 es comúnmente llamado "Ethernet grueso", esta especificación es el estándar 802.3 original. La primera etiqueta, "10" , especifica la velocidad a la que opera el medio (10 Mbps), la palabra "Base" se entiende por "Baseband", únicamente las señales Ethernet son transmitidas en el medio de comunicación (bus). La última etiquete "5", indica que la máxima longitud permitida en segmentos individuales de cable coaxial grueso es de 500m con un máximo de 100 nodos por segmento.

La longitud de la red puede ser extendida utilizando repetidores. El estándar permite un máximo de cuatro repetidores entre la ruta de nodos cualquiera, extendiendo la ruta efectiva de la red a una longitud de 2.5 Km. La conexión se hace por medio de una unidad llamada MAU (Médium Attachment Unit) conocido técnicamente como transceiver en el original estándar de Ethernet. Se le da este nombre debido a que recibe y transmite señales entre el medio Ethernet o segmento de red y la interfaz Ethernet.

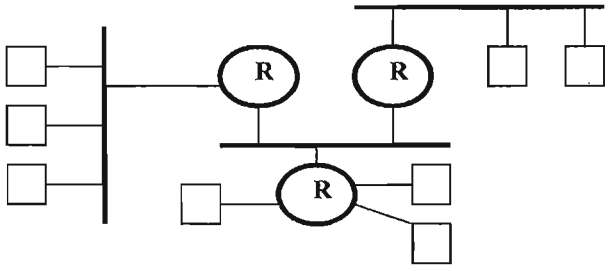


Figura 3.4 Configuración de una red Ethernet

10Base2

El segundo tipo de cable es el 10Base2 o "Ethernet delgado". El 2 es el valor redondeado de 185m. como longitud máxima de segmentos individuales de cable 10Base2. Las conexiones se hacen usando conectores BNC estándar de la industria para formar uniones T, en lugar de usar derivaciones vampiro. El Ethernet delgado es mucho más barato y más fácil de instalar, pero solo puede extenderse 200 metros con un máximo de 30 nodos por segmento de cable. La versión de 10Base2 es también conocida como Cheapernet.

10BaseT

Los problemas asociados con la localización de rupturas en el cable coaxial han llevado a un patrón de alambrado distinto, en la que todas las estaciones tienen alambres que conducen a un concentrador (hub) central. Generalmente, estos alambres son cables telefónicos en pares trenzados. Este esquema es conocido como 10BaseT, en la que se especifica una versión de operación con cable par trenzado sin blindar UTP operando a 10Mbps utilizando un alambrado de estrella o una topología de concentrador.

Las estaciones conectadas punto a punto al repetidor multipuertos lo hacen por medio de dos pares de par trenzado, cada par de alambres forma un segmento de enlace, uno de transmisión y otro de recepción. La tasa de transmisión de datos es de 10Mps utilizando codificación Manchester. Con 10BaseT no hay cable en absoluto, solo el concentrador (hub). Agregar o remover estaciones es sencillo con esta configuración, y las rupturas del cable pueden detectarse con mayor facilidad. La desventaja de 10BaseT es que la longitud máxima del cable es de únicamente 100 metros y hasta 150 metros si es utilizado un par trenzado de mayor calidad (categoría 5). Como una alternativa, un enlace de fibra óptica puede ser utilizado. En este caso, la longitud máxima es de 500 metros.

En el sistema 10BaseT , todos los repetidores multipuestos funcionan de la misma manera como un repetidor ordinario de los sistemas 10Base5 y 10Base2. Una ventaja de utilizar repetidores y el uso de la tasa de transmisión de datos a 10Mps es que el sistema 10BaseT pude ser mezclado con los sistemas 10Base5 y 10Base2.

Existen dos reglas de configuración para más de un concentrador conectado a una red Ethernet, las cuales son: Un máximo de cuatro concentradores en la ruta de envío de datos entre dos estaciones cualesquiera conectadas en la red, y los segmentos del cable UTP no deberá exceder la longitud de 100 metros.

Se consideran cinco segmentos de cable y un conjunto de cuatro repetidores como una ruta de transmisión máxima entre dos estaciones cualquiera. Un segmento es uno de los dos siguientes: segmento de enlace punto a punto o un segmento coaxial 10Base2 o 10Base5. El número máximo de segmentos de cable coaxial en una ruta es de tres segmentos.

10BaseF

Otra opción de cableado en el 802.3 es 10BaseF, que usa fibra óptica para redes Ethernet, la cual es de uso frecuente para cubrir largas distancias (hasta 2km. entre repetidores). Es también de uso común para cableado (backbone) entre

edificios. Esta alternativa resulta costosa debido al alto costo de los terminadores y conectores (es difícil que se llegue a instalar para la conexión directa entre las estaciones por el alto costo que representa el cableado con fibra óptica).

10BaseF utiliza la transmisión de datos por medio de pulsos de luz y no por medio de corriente eléctrica, lo que implica que tiene una excelente inmunidad contra el ruido. Mientras que el equipo Ethernet usado en segmentos de medio metálico tiene solamente protección de circuitos diseñado para riesgos eléctricos internos, el medio de la fibra óptica es totalmente no conductivo. Este completo aislamiento eléctrico provee inmunidad para un mayor número de riesgos eléctricos, incluyendo el efecto llamado "lighting strikes", de los diferentes niveles de corriente de tierra eléctrica que pueden ser encontradas en la conexión de instalaciones separadas.

Las ventajas que también se presentan con 10BaseF es la enorme distancia a la que puede extenderse un segmento de fibra óptica (2000 metros), además de que soporta velocidades de transmisión mayores de 10Mbps, por lo que la actualización de todo el sistema de cableado para alcanzar velocidades de transmisión mayores, no es necesario cambiar el esquema de cableado del backbone de fibra óptica o el cableado basado en ésta.

Los estándares 10BaseF y FOIRL

El enlace entre segmentos comúnmente se hace con el medio de fibra óptica. Existen dos tipos de enlace entre segmentos con fibra óptica, el segmento original Fiber Optic Inter-Repeater Link (FOIRL) y el segmento 10BaseFL. La especificación original FOIRL establece un segmento de hasta un kilómetro de distancia entre dos repetidores únicamente.

El conjunto de estándares conocidos como 10BaseF, incluyen especificaciones para un segmento de enlace con fibra óptica que permite conectar directamente a estaciones. Este conjunto completo de especificaciones 10BaseF incluye tres tipos de segmentos:

- **10BaseFL**. Este estándar reemplaza las anteriores especificaciones FOIRL, y fue diseñado para inter operar con el equipo basado en FOIRL existente. 10BaseFL establece un segmento de enlace de fibra óptica de hasta dos kilómetros de longitud, previendo que solamente equipo 10BaseFL sea utilizado en el segmento. Si se combinan 10BaseFL con equipo basado en FOIRL, entonces la longitud máxima disminuye a un kilómetro por segmento. Un segmento 10BaseFL puede ser conectado entre dos estaciones, dos repetidores o entre una estación y un puerto de repetidor.
- **10BaseFB**. Este estándar describe un segmento de cableado principal (backbone) de señal síncrona que permite que el límite de número de

repetidores que pueden ser usados en un sistema Ethernet a 10Mbps pueda ser excedido. Típicamente los enlaces 10BaseFB realizan la conexión entre concentradores repetidores, y son usados para enlazar concentradores repetidores de señal síncrona 10BaseFB especiales, juntos en un sistema de cableado principal (backbone) repetido que puede expandirse hasta dos kilómetros de longitud.

- **10BaseFP**[12]. El sistema de fibra pasiva establece un conjunto de especificaciones para un segmento combinado de fibra óptica que enlaza múltiples estaciones sobre un sistema de medio de fibra sin el uso de repetidores. Los segmentos 10BaseFP pueden alcanzar hasta 500 metros de longitud. El uso de un solo empalme en estrella pasiva de 10BaseFP puede enlazar hasta 33 estaciones.

Extensión de redes Ethernet con concentradores

Para lograr expandir una red Ethernet, los distribuidores de dispositivos de interconexión ofrecen los concentradores (hub) los cuales cuentan con múltiples puertos Ethernet. Un concentrador se establece como el elemento central en el sistema de cableado en bus de manera interna. Hay dos clases principales de concentradores: concentradores repetidores y concentradores conmutadores.

Cada puerto de un concentrador repetidor realiza una conexión individual de segmento de medio Ethernet, la estructura del concentrador une estos enlaces individuales para crear una gran red que opera como una sola red de área local Ethernet. Todos los segmentos y repetidores en la red LAN Ethernet deberán conocer las especificaciones del tiempo de viaje redondo de una señal (RRT). Los concentradores conmutadores establecen un esquema de conmutación de paquetes, típicamente basado en un esquema de puertos de puente.

Lo importante de cada puerto de un concentrador conmutador es que cada uno establece una conexión a un sistema de medio Ethernet que opera como una red Ethernet separada o independiente de las otras (un dominio de colisión por cada puerto, es decir, cada puerto tiene un ancho de banda de 10Mbps). La diferencia con un concentrador repetidor es que este combina puertos individuales como segmentos, al combinar segmentos conjuntamente para crear una sola LAN extensa (todo el esquema del concentrador repetidor es un dominio de colisión, es decir, todo esquema del concentrador repetidor con todos los segmentos que une y comparte el ancho de banda de 10Mbps). Un concentrador conmutador hace posible la división la división de un conjunto de sistemas de cableado Ethernet dentro de múltiples LANs que son enlazadas por medio de los componentes electrónicos de conmutación de paquetes dentro del concentrador. Las reglas de

[12] Este sistema no ha sido ampliamente adoptado desde su creación y el equipo no está disponible por distribuidores.

tiempo de viaje redondo (RTT) para cada LAN llegan hasta el puerto del concentrador conmutador, lo cual permite enlazar un gran número de redes LAN Ethernet individuales como una sola.

Mientras que una res LAN Ethernet individual puede generalmente soportar alunas docenas de estaciones, el sistema total de redes LAN Ethernet enlazado por medio del mecanismo conmutación de paquetes puede soportar varios miles de cientos de estaciones.

IEEE 802.3u Ethernet Rápido (Fast Ethernet)

Este es un agregado del estándar 802.3, el concepto de Ethernet Rápido (Fast Ethernet) es el de mantener todos los formatos de paquetes, interfases y reglas de procedimiento de Ethernet, y simplemente reducir el tiempo de bit de 100nseg, logrando con esto una velocidad de transmisión de 100Mbps. Se especifican tres tipos de medios para la transmisión de señales Fast Ethernet, los cuales se presentan en la siguiente tabla:

	100BaseT4	100BaseTX	100BaseF
Medio de Transmisión	Par trenzado (UDP) categoría 3,4 y 5	Par trenzado (UDP O STP) categoría 5	Fibra Óptica
Tasa de transmisión de Datos (Mbps)	100	100	2 fibras de 62.5/125 micrones multimodo
Características Principales	Para voz o grado De datos (Half Dúplex)	Para datos (Half o Full Dúplex)	Half o Full dúplex
Segmentos máximos	100 m	100m	2000m
Ventajas	Usa UTP Categoría 3	Dúplex integral a 100 Mbps	Dúplex integral a 100Mbps; soporta tramos grandes

Tabla 3.3 Medios de transmisión para Fast Ethernet

El esquema UTP categoría 3, llamado 100BaseT4, usa una velocidad de señalización de 25Mhz, sólo 25% más rápida que los 20Mhz del estándar 802.3. La etiqueta 100 es por la velocidad de transmisión de 100Mbps, Base se entiende por una señal banda base y la tercera etiqueta es un identificador del tipo de segmento. El tipo de segmento "T4" es un par trenzado que utiliza cuatro pares trenzados, un par va al concentrador, uno más viene del concentrador y los otros dos son conmutables a la dirección actual de transmisión. Para la transmisión de datos no se utiliza codificación Manchester, se envían señales ternarias con tres pares trenzados en la dirección de transmisión, puede transmitirse cualquiera de

27 símbolos, posibilitando el envío de 4 bits con redundancia. La transmisión de 4 bits en cada uno de los 25 millones de ciclos de reloj por segundo da los 100Mbps necesarios; este esquema en conocido como 8B6T (mapa de 8 bits a 6 ternas).

En el esquema 100BaseTX, los alambres pueden manejar tasas de reloj de hasta 125 Mhz o más. El tipo de segmento "TX" es un par trenzado que utiliza dos pares trenzados por estación, uno al concentrador y uno propio. Se utiliza un esquema de codificación llamado 4B5Ba 125Mhz. Cada grupo de 5 periodos de reloj se usa para enviar 4 bits a fin de tener cierta redundancia, proporcionar suficientes transiciones para permitir una fácil sincronización de los relojes, crear patrones únicos para delimitar paquetes y ser compatible con la FDDI en la capa física. El sistema 100BaseTX es un sistema dúplex integral, las estaciones pueden transmitir a 100Mbps y recibir a 100Mbps al mismo tiempo. El esquema 100BaseF utiliza dos hilos de fibra óptica multimodo, uno para transmitir y otro para recibir, por lo que se considera también un sistema dúplex integral con 100Mbps en cada dirección.

IEEE 802.3Z Gigabit Ethernet

Este es un agregado al estándar 802.3, donde se especifica la versión mas reciente de Ethernet, Gigabit Ethernet, la cual ofrece un acho de banda real de 1000Mbps (1Gbps), que es cien veces más rápido que el Ethernet original. Gigabit Ethernet mantiene todos los formatos de paquetes, interfases y reglas de procedimiento de Ethernet.

La capa física de Gagabit Ethernet es una mezcla de tecnologías comprobadas para el Ethernet original (802.3) y el ANSI X3T11 Especificación de Canal de Fibra. Gigabit Ethernet soporta cuatro tipos de medios definidos en el estándar 802.3ab (1000Base-T) y el 802.3z (1000Base-X). El medio 1000BaseX está basado en la Capa Física del Canal de Fibra, el cual es una Tecnología de interconexión en estaciones de trabajo, supercomputadoras, dispositivos de almacenamiento y periféricos. El Canal de Fibra tiene 4 capas de arquitectura. Las dos más bajas capas FC-0 (Interface y media) y FC-1 (Codificación/Decodificación) son usadas en Gigabit Ethernet. Los tres tipos de media especificados en 1000BaseX son:

- 1000Base-SX 850nm láser en fibra multimodo.
- 1000Base-LX 1300nm láser en fibra modo simple y multimodo.
- 1000Base-CX Short haul copper "twinax" STP cable.

En la siguiente tabla se presentan las distancias que soportan los tipos de medio 1000BaseX:

Tipo de medio	Distancia
Fibra modo simple (9micron)	300m. Utilizando 1300mm láser (LX)
Fibra multimodo (62.5micron)	300m. Utilizando 850nm laser (SX) 550m. Utilizando 1300nm laser (LX)
Fibra miltimodo (50micron)	550m. Utilizando 850nm laser (SX) 550m. Utilizando 1300nm láser(LX)
Short Half Copper	25m.

Tabla 3.4 Tipos de medios para 1000Base X y distancias

Para 1000BaseT el tipo de medio es par trenzado sin blindar (UTP) Long Haul Cooper (cuatro pares de UTP categoría 5) que soporta una distancia de 100 metros.

3.3.6. IEEE 802.4 Token Bus

El estándar 802.4 describe una red de área local llamada token bus (busca de ficha). El token bus es físicamente un cable lineal o en forma de árbol al que se conectan las estaciones. Las estaciones están organizadas lógicamente en forma de anillo, donde cada estación conoce la dirección de las estaciones en sus extremos de conexión. Cuando se inicializa el anillo lógico, una estación puede enviar el primer paquete. Al término de esto, para el permiso a su vecino inmediato enviándole un paquete de control especial llamado token (testigo). El testigo se propaga alrededor del anillo lógico, teniendo permiso de envío de paquetes aquel que tenga el testigo. Debido a que únicamente una estación puede enviar paquetes a la vez, no existen colisiones. Una característica importante de una red token bus es que no importa el orden físico en que están conectadas las estaciones en la red debido a que el cable es inherentemente un medio de difusión, todas las estaciones reciben todos los paquetes descartando aquellos que no sean dirigidos a ellas.

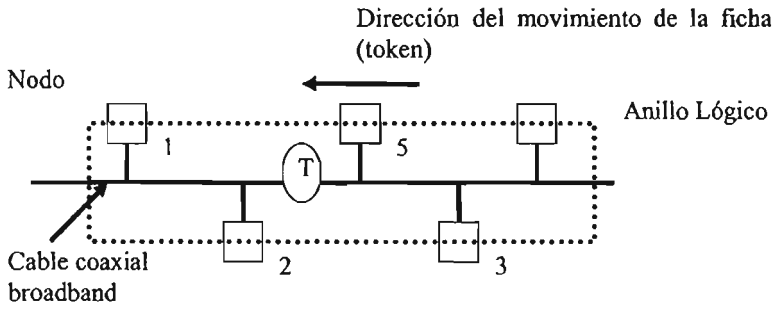


Figura 3.5 Token Bus

Normalmente en la implementación de una red token bus se utiliza cable coaxial de 750hms como medio de transmisión el cual opera en modo broadband o u modo de baseband modificado conocido como carrierband13.

Al igual que el baseband el carrierband utiliza todo el ancho de banda del cable en una transmisión, la diferencia en que el modo carrierband modula los datos antes de ser transmitidos. Para la capa física Token Bus14 especifica tres opciones:

1. Sistema Broadband. Este sistema soporta canales de datos a 1, 5 y 10Mbps con anchos de banda de 1.5, 6 y 12 Mhz respectivamente. El estándar recomienda el uso de un sistema divido de un solo cable con un traductor de frecuencia principal (la configuración de cable dual o doble también es permitida).
2. Carrierband o broadband de u solo canal (single-channel Broadband). El esquema corrierband especifica las tasas de transmisión de 1, 5 y 10Mbps.
3. Fibra Óptica. En este sistema se especifican tres tasas de transmisión: 5, 10 y 20Mbps.

[13] Una señal carrierband significa que el espectro total del cable es dedicado una sola dirección de transmisión en el caso de las señales analógicas.

[14] Es importante mencionar que no es frecuente la implementación de redes LAN en token bus, su mayor aplicación e sen industrias de manufactura, es decir, fábricas automatizadas con el control de procesos.

En la siguiente tabla se muestran las opciones para la capa física del estándar 802.4:

	Broadband	Carrierband de Fase continua	Carrierband de Fase coherente	Fibra óptica
Tasa de Transmisión (Mbps)	1 5 10	1	5	5, 10, 20
Ancho de Banda	1.5Mhz 6Mhz N/A	N/A	N/A	270nm
Centro de Frecuencia	1.5Mhz - -	5Mhz	7.5Mhz	800-900nm
Modulación	Multinivel duobinary AM/PSK	Manchester/fase Continua FSK	Fase Coherente FSK	On-Off
Topología	Bus direccional (árbol)	Bus (omnidireccional)	Bus (omnidireccional)	Estrella pasiva o activa
Medio de Transmisión	Cable coaxial 75 Ohms	Cable coaxial 75 Ohms	Cable coaxial 75 Ohms	Fibra óptica

Tabla 3.5 Medios de transmisión para el estándar 802.4

3.3.7. IEEE Token Ring

La característica principal de una red en anillo es que realmente no es un medio de difusión, sino un conjunto de enlaces punto a punto que llegan a formar un círculo. Una red en anillo también es equitativa y tiene un límite conocido como acceso al medio. IBM escogió el anillo como su LAN y el IEEE lo incluyó como el estándar token ring.

Las redes locales token ring son conexiones punto a punto donde cada estación actúa como un repetidor, regenerando la señal y corrigiendo errores en esta. Alrededor del anillo circula un patrón de bit especial, llamado token (testigo). En el momento en que una estación quiere transmitir paquetes de información, debe tomar el token y retirarlo del anillo antes de transmitir. Esta es la manera de resolver el control de acceso al medio al igual que lo resuelve token bus. En el momento en que la estación transmisora ha terminado de enviar el último bit de su último paquete, debe de regenerar el token para que esté disponible para otras estaciones en la red.

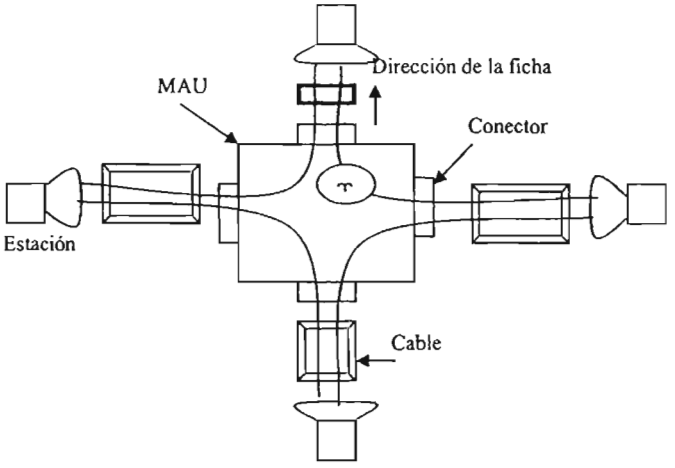


Figura 3.6 Token Ring

El uso de la tecnología ASIC es la que permite al swich dar un mayor desempeño que un bridge tradicional dando una lata cantidad de manejo de paquetes con un retardo extremadamente pequeño. Esto permite al switch el manejo simultáneo de reenvío de paquetes a través de todos los puertos a la velocidad de que el cable pueda brindar. Como se menciono en el capitulo anterior acerca de las desventajas que presentan cada una de las topologías de red; en el caso del anillo Una de las desventajas del anillo es que se inhabilita por completo la red cuando el canal de comunicación sufre un daño en cualquier parte. En una red loca token ring puede solucionarse este problema cableado los nodos a una unidad de acceso múltiple central (concentrador MAU) que repite las señales de una estación a la siguiente. Las unidades de acceso múltiple (MAU-Multistation Access Unit) se cablean conjuntamente para extender la red, lo cuál implica el anillo lógico.

La tecnología de redes en anillo es casi completamente digital, en contraste con 802.3 que tiene una componente analógica considerable para la detección de colisiones (CSMA/CD). El tiempo de respuesta en redes en anillo es determinístico aún en condiciones de carga pesada en le red.

El tamaño mínimo de un anillo deberá ser de un kilómetro, este tamaño es muy extenso en el caso de que se quiera conectar pocas estaciones, por esta razón, se instala una estación especial designada como "monitor activo", el cual ocasionará un retraso de almacenamiento de 24 bits para el anillo. Este almacenamiento también compensa cualquier fase jitter acumulada sobre el anillo. El monitor activo no es una estación con dispositivos de red especial, cualquier estación sobre el

anillo puede ser monitor activo y las demás estaciones designadas como pasivas. La selección de la estación se lleva a cabo en el procedimiento de inicio del anillo.

Los enlaces en una red token ring pueden ser cualquier tipo de medio, cable coaxial, par trenzado operando a 1, 4 y 16[15] Mbps y fibra óptica (básicamente se utilizan para extender la red sobre grandes distancias). Las señales se codifican usando codificación Manchester diferencial, siendo las señales positivas y negativas de magnitudes absolutas de 3.0 a 4.5 Volts. La configuración de 1 Mbps utiliza cable par trenzado sin blindar (UTP), las configuraciones de 4 y 16 Mbps soportan cable par trenzado blindado (STP) y par trenzado sin blindar. En la siguiente tabla se muestran las reglas de cableado para redes token ring:

Parámetros de token ring	**Tipo 1 y Tipo 2**	**Tipo 3**
Núm. Máximo de dispositivos por anillo	260	96
Núm. Mínimo de dispositivos por anillo	2	2
Tasa de transmisión	16 Mbps	4 Mbps
Estación a una sola MAU LAN	300 metros	100 metros
Estación a múltiples MAU LAN	100 metros	45 metros
Máximo número de MAUs por LAN	12	2
Distancias entre MAUs	200 metros	120 metros

Tabla 3.6 Reglas de cableado para redes token ring

En las especificaciones para el cable tipo 1 y tipo2 se establece un máximo de 260 dispositivos por anillo aunque se recomienda un número alrededor de 100. El número mínimo de estaciones para tener un anillo utilizable es de dos.

La distancia máxima entre una estación y el MAU (Multistation Access Unit) es de 300 metros. Podemos mencionar que el estándar X3T9 referente a la Interfaz de Datos Distribuidos por Fibra (FDDI-Fiber Distributed Data Interface) está basada en el estándar 802.5 Token Ring, X3T9 fue desarrollado por el comité de normas acreditadas (ASC- Acredited Standars Commitee).

[15] La versión de 16 Mbps fue introducida posteriormente por IBM

3.3.8. IEEE 802.6 Red de Área Metropolitana

Para redes que cubren toda una ciudad, redes de área metropolitana (MAN), el IEEE definió un protocolo de alta velocidad llamado bus doble de colas distribuidas (DQDB – Distributed Dual Bus).

Las estaciones se enlazan compartiendo dos buses unidireccionales de fibra óptica que se extiende a través de toda una ciudad. Estos buses ofrecen tolerancia a fallas para mantener activas las conexiones en los casos en que se presente una ruptura o falla del bus. Cada bus tiene una cabeza terminal (head-end), el cual es un dispositivo que inicia la transmisión de datos. Cada cabeza terminal genera una cadena constante de células de 53 bytes, cada célula viaja corriente abajo del head-end y cuando llega al final, sale del bus. Cada célula tiene un campo de 44 bytes de carga, lo que la hace compatible con algunos modos de capa AAL[16] (ATM Adaption Layer, capa de adaptación de ATM) en redes ATM (Asynchronous Transference Mode). Cada célula contiene también dos bits de protocolo ocupado, que se establece para indicar que la célula está ocupada, y solicitud, que puede establecerse cuando una estación quiera hacer una solicitud.

En la norma MAN, se designa para proporcionar servicios de datos, voz y video en un área metropolitana de aproximadamente 50 kilómetros, con una velocidad de transmisión de datos (células) de 1.5, 45 y 155 Mbps. Los servicios MAN son orientados a conexión y no orientados a conexión, y (o) isócronos (video en tiempo real). El bus tiene una serie de ranuras de longitud fija donde se sitúan los datos para su transmisión sobre el bus. Así, cualquier estación que necesite transmitir, únicamente sitúa los datos en una o más ranuras. Para situar datos isócronos sensibles al tiempo, se reservan unas ranuras a intervalos regulares para garantizar que los datos lleguen a tiempo y en secuencia.

3.3.9. IEEE 802.7 Grupo asesor para técnicas de banda ancha

El propósito de este subcomité es la de proporcionar soporte y consejos técnicos a otros subcomités en el área de conexiones de redes de banda ancha.

3.3.10. IEEE 802.8 Grupo asesor para técnicas de fibra óptica

Este subcomité ofrece soporte a otros subcomités para redes que utilizan fibra óptica como alternativa de medio de transmisión a las redes actuales basadas en cable de cobre.

[16] La ITU (Unión Internacional de Telecomunicaciones) definió la capa AAL con el fin de proporcionar servicios útiles a programas de aplicación evitando el procedimiento de dividir datos en células en el origen y reorganizándolos en el destino.

3.3.11. IEEE 802.9 Redes integradas por voz y video

El subcomité 802.9 del IEEE se encarga de la integración de tráfico de datos, voz y vedio en redes de área local 802.x y en redes digitales de servicios integrados 8ISDN, Integrated Services Digital Networks). En las especificaciones de este comité definen como nodos a computadoras, teléfonos, codificadores y decodificadores (codec) de video. Estas especificaciones son conocidas como IVD (Integrated Voice and Data). El servicio proporciona un flujo multiplexado que puede llevar señales de voz y datos por los canales que en lazan las dos estaciones sobre canales de par trenzado de cobre. Se definen varios tipos distintos de canales entre los que se incluyen los canales dúplex no conmutados a 64bps, de conmutación de circuitos o de conmutación de paquetes.

3.3.12. IEEE 802.10 Seguridad en red

Este subcomité el IEEE trabaja en la definición de un modelo de seguridad que opera sobre distintas redes incorporando métodos de autentificación y cifrado.

3.3.13. IEEE 802.11 Redes Inalámbricas

El subcomité 802.11 del IEEE se encarga de establecer las normas a seguir para redes inalámbricas que se basan en medios como los rayos infrarrojos, transmisiones sobre líneas de potencia, radio de banda estrecha y la radio de espectro expandido. Otra área de trabajo de este subcomité es la normalización de interfaces inalámbricas para redes informáticas como lo son sistemas formados por computadoras que se basan en lápices, asistentes digitales personales (PDS, Personal Digital Assistants) y otros dispositivos portátiles.

Para las redes inalámbricas se plantearon dos enfoques, el planteamiento distribuido y el planteamiento de punto de coordinación. El planteamiento de punto de coordinación está basado en el uso de un concentrador central, perteneciente a una red cableada, que controla las transmisiones de las estaciones inalámbricas. El planteamiento distribuido se basa en que cada estación controla su acceso a la red.

3.3.14. IEEE 802.12 LAN de acceso de prioridad por demanda -100VG AnyLAN

Este subcomité define las normas de la primera red Ethernet que opera a 100Mbps con el método de acceso de prioridad por demanda (Demand Priority Access Method) originalmente desarrollado por Hewlwtt Packard. 100VG (Voice Grade) AnyLAN es una tecnología de red que combina elementos de Ethernet y Token Ring. Las especificaciones del 802.12 son establecidas en base a la

transmisión de paquetes Ethernet (802.3) y paquetes Token Ring (802.5). El medio de transmisión especificado es par trenzado categoría 3, 4 y 5, y fibra óptica además de soportar una topología de estrella en cascada.

El método de acceso de prioridad por demanda únicamente utiliza dos niveles de prioridad, alta o baja. Utiliza un concentrador central para controlar el acceso al canal de comunicación compartido. Las prioridades están disponibles para soportar la distribución de la información de aplicaciones que utilizan un gran ancho de banda en tiempo real, aplicaciones como video, CAM (Computer Arded Manufacturing) y CAD (Computer Arded Design).

3.3.15. IEEE 802.14 Cable de T.V.

Este subcomité tiene asignada la tarea de crear normas para el transporte de datos sobre el tradicional cable de TV en redes. La referencia de la arquitectura especifica es una planta híbrida, de cable coaxial y fibra óptica 8HFC, Irbid Fiber Coax) con un radio de 80 kilómetros a partir de una cabeza terminal (head-end).

Las especificaciones del 802.14 establecen un protocolo de control de acceso al medio en el que se identifican tres características: sincronización, resolución a colisiones y una capa de intervalo de resolución de colisiones (CRI). Se trata de establecer que exista soporte para aplicaciones multimedia sobre HFC y compatibilidad con diversas tecnologías como ATM, así se especifica el soporte para el tamaño de las células de una red ATM y para los diversos tamaños de paquetes de información en otras tecnologías de red; además de existir reservación de acceso al medio y acceso isócrono.

3.3.16. IEEE 802.15 Redes Inalámbricas de Área Personal

El grupo de trabajo de IEEE 802.15 establece normas para redes inalámbricas de área personal (WPANs) las cuales se aplican en prácticas de telecomunicaciones, el intercambio de información entre redes locales y redes de área metropolitana, y redes inalámbricas de área personal que operan en una banda de frecuencia no autorizada.

Una red inalámbrica de área personal, o WPAN, es un esquema de red de trabajo de bajo costo que permite a dispositivos como computadoras personales, computadoras laptop, impresoras y asistentes personales digitales (PDAs, Personal Digital Assistants) comunicarse entre sí en distancias cortas, sin la existencia de cableado.

Un área de desarrollo del 802.15 llamada Práctica Recomendada (Recommended Practice) se encarga de normalizar la coexistencia de una WPAM con un sistema WLAN (Gíreles Local Area Networks) 802.11 operando a una misma banda de

frecuencia. Otra área de trabajo llamada Actividad iniciada (Initiate Activity) se encargará de guiar al estándar 802.15 a un alto rango de transmisión de datos en uan WPAN a bajo costo, los datos pueden ser transmitidos de manera organizada en rangos cortos por medios inalámbricos, particularmente para aplicaciones multimedia. Además de IEEE, Motorota, Eastman Kodak y Cisco trabajan en este proyecto.

3.4. Estándares de Cableado Estructurado

Antes de 1984 se hablaba poco de los sistemas de cableado para comunicaciones. Las grandes gerencias al tomar decisiones importantes no tomaban en cuenta los cableados que iban a estar detrás de sus paredes. La compañía de teléfonos movía, agregaba y cambiaba los equipos y cobraba una tarifa por instalar cada artículo. Cuando el procesamiento de datos se descentralizó y se instaló en las oficinas, el cableado lo realizaban los fabricantes de los equipos, entonces se agregaba al costo del equipo la conexión de este.

Originalmente, la libertad de elección de un medio de telecomunicación causó confusión y debida a esta, algunos organizaciones como TIA (Telecommunication Institute American) se vieran obligados a ponerse al día con respecto a sus normas. Surgieron dudas de la capacidad de desempeño de los diversos materiales de comunicación, los límites de las longitudes, la topología más apropiada y si se cumplirían los requisitos de los sistemas una vez que se combinaran los componentes individuales. A medida que los usuarios y los grupos de usuarios se esforzaban en responder las preguntas que se hacían, se hizo evidente que había que desarrollar un método estándar para la instalación del cableado de comunicaciones, método que se designó como cableado estructurado.

El sistema de cableado soportará un ambiente multiproductos y multiproveedor. Esto implica que debe se lo más general posible. Es decir, no se trata de diseñar un cableado teniendo en cuenta la utilización que se le dará en el corto plazo, sino tratando en lo posible de que sea independiente de los productos que lo utilizarán y de la disposición y uso de las oficinas. Un sistema de cableado estructurado debe caracterizarse por ser:

- **Fiable**, en el sentido de no tener interrupciones o caídas continuas de la red que este conectada por el, además de no tener problemas como atenuaciones de la señal, diafonías, etc.
- **Flexible**, permitiendo el fácil cambio de los servicios y de los mismos usuarios, así como la implementación de diversos servicios de voz, datos y video.
- **Modular**, que pueda ser fácilmente configurable según las necesidades cambiantes de la empresa.

- **Integrador de servicios**, ya que en un mismo cableado se puede tener diversos servicios.
- **Sencillo de administrar** por medio de un software comercial de gestión de redes.

Estos requerimientos permiten tener beneficios, que un cableado estructurado cumple con estándares fijados por la industria, tiene una aplicación independiente del tipo de servicio a usar por el sistema, abre la conectividad de distintos equipos, soporta la alta velocidad de las nuevas tecnologías de las redes, y todo esto a un costo relativamente bajo a lo obtenido. El cableado estructurado brinda la facilidad de usar un solo tipo de cable par todos los servicios de comunicaciones, lo que resulta en un abaratamiento y una total estandarización de la red.

Al usarse un solo tipo de cable, un usuario se desplaza a cualquier lugar del edificio ya que la conexión necesaria se realizará en unos cuantos minutos. Cuando se planee conectar o instalar nuevos equipos, no se tendrá necesidad de tener nuevos cables con un sistema estructurado, estos ya estarán tendidos y funcionaran con cualquier sistema estructurado.

Por estas razones, el sistema debe ser diseñado e instalado de tal forma que permita las modificaciones y ampliaciones necesarias para soportar cualquier tipo de comunicación (actual y futura) además de ser lo suficientemente flexible para acomodarse a las novedades tecnológicas, todo esto sin nuevas tiradas de cable. El período de vida útil a considerar es de doce a quince años como mínimo.

Esta filosofía de diseño se aplica principalmente en las instalaciones donde los usuarios y la densidad de comunicación por planta son lo suficientemente elevadas como para requerir movimientos de personal o equipo de comunicaciones de forma más o menos continua o la adaptación de nuevos equipos. Aplicada así, se permite la fácil reubicación de los usuarios o el equipo a un costo mínimo, con la consiguiente facilidad de administración y mantenimiento de la red. Dentro de la instalación se tiene en cuenta las recomendaciones internacionales:

- ANSI/TIA/EIA-568-A Commercial Building Telecomunicactions Wiring Standard.
- ANSI/TIA/EIA-569-A Commercial Building Standard for Telecommuncations Pathways and Spaces.
- ANSI/TIA/EIA-606-A The Administration Standard for the Telecommunications Infraestructure of Commercial Buildings
- ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecomunications.

Los que hacen referencia a:

- Características de los materiales empleados (especificaciones de los cables, conectores, cajas de conexión, etc.)
- Control de calidad de la instalación (métodos utilizados, separación de diferentes servicios, aislamiento a interferencias electromagnéticas, tomas de tierra, etc)
- Diseño y administración de la red (topologías soportadas, distancias críticas del cableado, códigos de color de los cables, etiquetado, documentación final, etc.)

3.4.1. ANSI/TIA/EIA-568-A
Estándar de Cableado para Telecomunicaciones en Edificios Comerciales

Este estándar especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que pueda soportar múltiples ambientes de productos y fabricantes. El propósito de este estándar es establecer la planeación e instalación de un sistema de cableado en edificios comerciales. Este estándar establece criterios técnicos para distintas configuraciones de sistemas de cableado, para sus interfaces y la conectividad entre sus respectivos elementos.

La figura 3.7 muestra un sistema típico de cableado para telecomunicaciones, así como los elementos funcionales que lo comprenden y su relación e interfaces correspondientes, aunque no precisamente debe seguirse esta estructura como se plantea debe considerarse como un ejemplo.

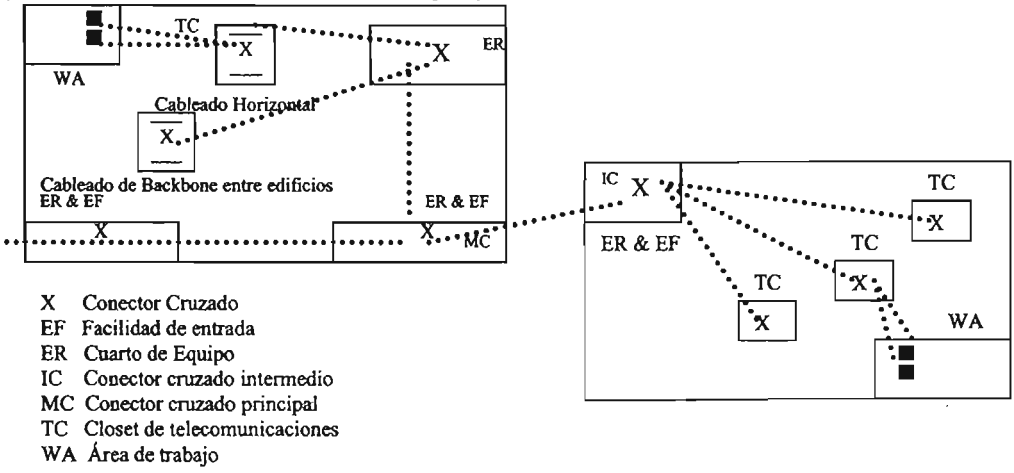


Figura 3.7 Sistema típico de cableado para telecomunicaciones

Los elementos que componen un sistema de cableado estructurado para telecomunicaciones son:

- **Cableado horizontal**
  El cableado horizontal es la porción del sistema de cableado para telecomunicaciones que se extiende desde los conectores para salida de telecomunicaciones (outlet/conecor) ubicados en el área de trabajo hasta los conectores-cruzados (cross-connected) que permiten la terminación de cable para su interconexión con el hardware de conexión (pach panel) en los closets de telecomunicaciones. El cableado horizontal incluye entonces: los cables horizontales, los conectores de salida para telecomunicaciones (outlet/conector) ubicados en el área de trabajo, las terminaciones mecánicas y el hardware de conexión (match coros o jumpers), localizados en los closets de telecomunicaciones. El cableado horizontal debe estar conectado en topología tipo estrella. Cada salida de telecomunicaciones en el área de trabajo debe de ir conectado a una terminación de cableado ubicada en el closet de telecomunicaciones, conocido como conector-cruzado horizontal (cross-connect). Una sola área de trabajo debe ser servida por un closet de telecomunicaciones, ubicados ambos en el mismo piso. La figura 3.8 muestra la topología típica para un cableado horizontal.

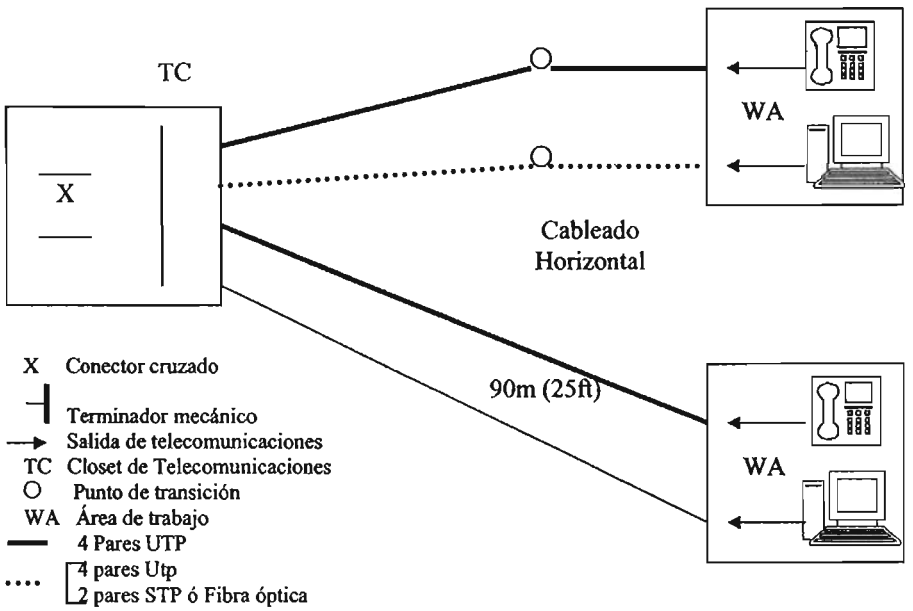


Figura 3.8 Topología típica del cableado horizontal

La distancia horizontal máxima debe ser de 90m independientemente del tipo de medio utilizado. Las limitaciones de distancia para los jumpers y match coros dentro de las facilidades de los crossconnect, incluyendo los cross-connect horizontales, jumpers y match coros que conectan el cableado horizontal con el equipo o al cableado de backbone, no debe exceder 6m de longitud. Son tres tipos de cables los reconocidos para el sistema de cableado horizontal:

- Par trenzado sin blindar de cuatro pares 100 (Ω)
- Par trenzado blindado de dos pares 150 (Ω)
- Fibra óptica de dos fibras, 62.5/125 (μm)

En ciertas ocasiones, el cable coaxial de 50 Ω es reconocido para emplearlo en el cableado horizontal, sin embargo, este no es recomendado para un sistema de cableado nuevo hasta futuras revisiones de este estándar.

➢ Cable de Backbone

La función del cableado de backbone es proveer interconexiones entre los closets de telecomunicaciones, cuartos de equipo y facilidades de entrada en la estructura del sistema de cableado de telecomunicaciones. El cableado de backbone está formado por los cables de backbone, las terminaciones del cable principal e intermedio (cross-connect), terminadores mecánicos y pach cords o jumpers usados para el esquema de conexión de backbone a backbone (cross-connection principal). El cableado de backbone también incluye el cableado entre edificios.

El cableado de backbone debe usar la topología convencional de estrella jerárquica como se ilustra en la figura 3.9, donde cada cross-connect horizontal en un closet de telecomunicaciones es cableado hacia el cross-connect principal o el cross-connect intermedio. No debe de haber más de dos niveles jerárquicos en el cableado de backbone, es decir, desde el cross-connect horizontal hacia el cross-connect principal no debe existir más de un cross-connect intermedio; solamente un cross-connect debe pasar a lo largo del cross-connect principal.

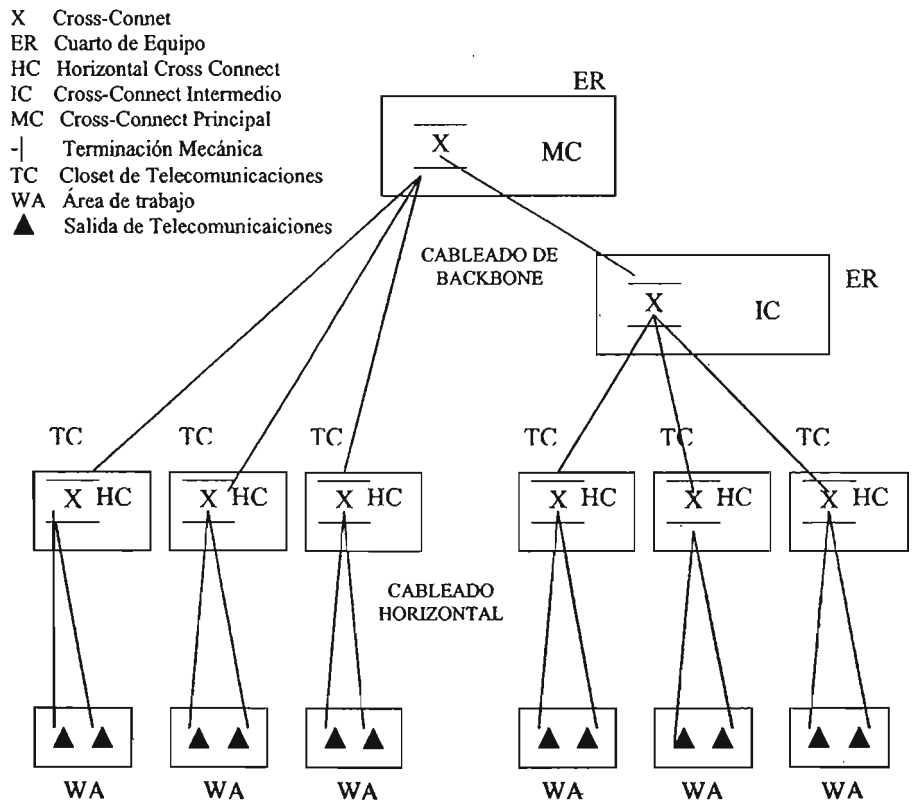


Figura 3.9 Topología en estrella jerárquica de cableado de backbone.

El cross-connect del cableado de backbone puede estar localizado en los closets de telecomunicaciones, cuartos de equipo o facilidades de entrada (acometida del cableado al edificio).

Los sistemas que están diseñados para una topología distinta a estrella como son topologías anillo, bus o árbol, pueden ser distribuidas como la topología mostrada anteriormente mediante el uso apropiado de interconexiones electrónicas o adaptadores en el closet de telecomunicaciones. Si los requerimientos para las configuraciones de bus o anillo son anticipados, el cableado directamente entre los closets de telecomunicaciones es permitido, debido al amplio rango de servicios y tamaños de sitios para los cuales el backbone puede ser utilizado, más de un medio de transmisión es reconocido para este.

Estos medios pueden ser usados individualmente o en combinación de los mismos. Los medios reconocidos son:

- Cable UTP de 100 (Ω)
- Cable STP de 150 (Ω)
- Fibra óptica de 62.5/125 (μm)
- Fibra óptica mono modo (single-mode)

En ciertas ocasiones, el cable coaxial de 50 (Ω) es reconocido par emplearlo en el cableado horizontal, sin embargo, este no es recomendado par un sistema de cableado nuevo hasta futuras revisiones de este estándar.

El cableado de backbone debe ser aplicable a un rango amplio de requerimientos de usuario, por lo cual, dependiendo de las características de los servicios a proporcionar por el sistema de telecomunicaciones deberá realizarse la elección del medio para este cableado. Cada cable reconocido tiene características individuales que los hace muy útiles en situaciones variadas, por lo cual un sólo tipo de cable puede no satisfacer todos los requerimientos de usuario, entonces será necesario el uso de más de un medio en el cableado de backbone. En este caso, el medio distinto deberá usar la misma facilidad de arquitectura con la misma localización de cross-connect, terminaciones mecánicas, facilidades de entradas entre edificios, etc.

Las distancias máximas en el cableado de backbone dependen de la aplicación, para minimizar distancias se localizará el cross-connect principal cerca del centro del lugar. Instalaciones que excedan el límite de distancia pueden ser divididas en áreas, cada una de las cuales pueden ser soportadas por el cableado de backbone dentro de los alcances del estándar, esto se puede completar usando tecnologías y equipo normalmente usado en aplicaciones de área amplia.

Tipo de Medio	A	B	C
UTP	800 m (max)	500 m (max)	300 m
STP-A			
Fibra óptica	2000 m (max)	500 m (max)	1500 m (max)
Fibra óptica mono modo	3000 m (max)	500 m (max)	2500 m (max)

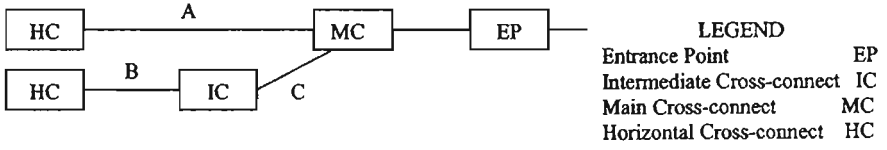


Figura 3.10 Distancias de cableado del Backbone

➢ **Área de trabajo**

Los componentes del área de trabajo se extienden desde el terminador de salida de telecomunicaciones del sistema de cableado horizontal hasta la estación de equipamiento, y están fuera de los alcances de este estándar. La estación de equipamiento puede ser cualquier número de dispositivos incluyendo pero no limitando teléfonos, terminales de datos y computadoras. El cableado en el área de trabajo es crítico para un buen desempeño de la distribución de sistemas.

La longitud máxima de cable horizontal se especificó ya anteriormente en las distancias del cableado horizontal con la consideración de que la longitud máxima de 3m del match cord ha sido usada en el área de trabajo

Los puntos importantes a considerar para el área de trabajo son detallados en el estándar ANSI/TIA/EIA-569, el cual será tratado más adelante.

➢ **Closet de telecomunicaciones**

El closet de telecomunicaciones provee diferentes funciones para el sistema de cableado y son tratadas como distintos subsistemas dentro del sistema de cableado jerárquico descrito en el cableado horizontal y en el cableado de backbone.

El closet de telecomunicaciones debe ser diseñado y acondicionado de acuerdo a los requerimientos en el ANSI/TIA/EIA-569. La función primaria de un closet de telecomunicaciones es la terminación de la distribución del cableado horizontal. Todos los cables reconocidos para el cableado horizontal están terminados en el closet de telecomunicaciones en hardware de conexión compatible. Similarmente, los cables reconocidos de backbone están también terminados en el closet de telecomunicaciones en hardware de conexión compatible. El esquema de conexión (cross-connection) del cable horizontal y de backbone usan jumpers o match cods que permiten la conectividad flexible cuando se extienden varios servicios hacia la salida de telecomunicaciones en el área de trabajo. El hardware de conexión, jumpers, y match cords usados para este propósito son colectivamente referidos al cross-connect horizontal. Un closet de telecomunicaciones puede también contener el cross-connect intermedios o bien el cross-connect principal para diferentes porciones del sistema de cableado de backbone. Un closet de telecomunicaciones también provee un ambiente controlado para el equipo de telcomunciaciones, hardware de conexión y terminadores de empalme que sirven a una porción del edificio. En algunos casos, el punto de demarcación y la protección asociada a algunos equipos puede esta localizada en el closet de telecomunicaciones.

➢ **Cuartos de equipo**

Los cuartos de equipo son considerados distintos de los closets de telecomunicaciones debido a la naturaleza o complejidad del equipo que en ellos se encuentre localizado. La mayoría o todas las funciones de un closet de telecomunicaciones pueden ser alternadamente previstas por un cuarto de equipo.

Los cuartos de equipo deben ser diseñados y acondicionados de acuerdo a los requerimientos del ANSI/TIA/EIA-569. Un cuarto de equipo provee un ambiente controlado al equipo de telecomunicaciones, hardware de conexión, terminadores de empalme, facilidades de unión de puesta a tierra y aparatos de protección donde sea aplicable. Desde la perspectiva de cableado, un cuarto de equipo contiene el cross-connect principalmente o bien el cross-connect intermedio usado en el cableado jerárquico del backbone. Un cuarto de equipo puede también albergar hardware de conexión (y pueden contener terminaciones horizontales para un porción del edificio). En muchos casos, el cuarto de equipo contiene la línea principal de terminadores o terminadores auxiliares que están bajo el control de las proposiciones de cableado del administrador.

➢ **Facilidades de entrada**

Las facilidades de entrada consisten de los cables, hardware de conexión, dispositivos de protección, y otros equipos necesarios para conectar las instalaciones externas necesarias de cableado. Esto componentes pueden ser usados por servicios de reces públicas, servicios de clientes de redes privadas o ambos. El punto de demarcación entre los proveedores de servicio y las premisas de cableado del cliente pueden ser parte de las facilidades de entrada. El proveedor debe ser contactado para determinar las políticas urgentes de localización en el área.

Las rutas y espacios de las facilidades de entrada deben ser diseñadas e instaladas de acuerdo con los requerimientos del ANSI/EIA/TIA-569. La protección eléctrica es gobernada por los códigos aplicables de electricidad. Los cables de backbone entre edificios y antenas pueden requerir dispositivos de protección. Las facilidades de entrada incluyen conexión entre cableados usando el ambiente exterior y el cableado autorizado para la distribución en el edificio. Los requerimientos de unión puesta a tierra están dados en el ANSI/TIA/EIA-607 que será visto posteriormente.

Las especificaciones de este estándar para la construcción del cableado para telecomunicaciones son con el fin de soportar un rango de diferentes edificios comerciales y servicios (voz, videos, datos, texto e imagen). Típicamente, este

incluye sitios con una extensión geográfica arriba de 3,000m, arriba de 1,000,000m^2 de espacio en oficinas y con una población superior a 50,000 personas.

3.4.2 ANSI/TIA/EIA-569-A

Estándar de rutas y espacios de telecomunicaciones para edificios comerciales.

Este estándar reconoce tres conceptos fundamentales relacionados a edificios y telecomunicaciones:

1. Las construcciones son dinámicas, es decir, que la remodelación en una construcción es más una regla que una excepción.
2. Los sistemas y el medio de telecomunicaciones en una construcción son dinámicos, es decir, que estos componentes pueden cambiar drásticamente, y
3. Las telecomunicaciones son más que datos y voz.

El propósito de este estándar se enfoca a la estandarización de un diseño específico y construcciones prácticas dentro y entre edificios. Es decir, la flexibilidad que proporcionan los espacios y rutas a través de los cuales el medio y equipo de telecomunicaciones es instalado. El alcance de este estándar está limitado al aspecto de telecomunicaciones, de diseño y construcción de edificios comerciales, en conjunto de las consideraciones de telecomunicaciones entre ambos y entre los edificios. Este estándar no estandariza el medio o equipamiento, solo estandariza las rutas y espacios dentro y entre construcciones en los cuales el medio y equipo de telecomunicaciones está localizado. Las telecomunicaciones tienen un gran impacto en la mayoría de las áreas internas y externas de construcciones comerciales. Por esto y otros factores adicionales la vida útil de una construcción debe ser de un lapso de varias décadas, es muy importante que el diseño y construcción de edificios nuevos o remodelados sean hechos evitando la obsolescencia.

A continuación se describen las características globales de los elementos básicos en un edificio.

- **Rutas horizontales (horizontal pathways)**

Estas "facilidades" proveen rutas para la instalación del medio desde el closet de telecomunicaciones hacia el conector de salida para el área de trabajo. Una "facilidad" de ruta horizontal puede estar formada de varios componentes incluyendo la charolo del cable, conductores, piso falso, piso de acceso, techo, y perímetros de sistemas.

Las facilidades de rutas, como mínimo, deben diseñarse tomando en cuanta todos los medios reconocidos en el ANSI/TIA/EIA-568-A , se deben determinar el tamaño y la cantidad de las rutas, el tamaño de los cables y los requerimientos del radio de curvatura, permitiendo un crecimiento futuro. Las rutas horizontales no deben estar localizadas en los ejes de los elevadores, y se deben acomodar de acuerdo a los requerimientos de zonas sísmicas.

Las rutas horizontales entre edificios deben ser instaladas en lugares secos para proteger los cables de niveles de humedad que entorpezcan los rangos de operación de las premisas del cable.

Dentro de las rutas bajo el piso se encuentran los ductos de diferentes niveles, esto considerando que los ductos de distribución del cableado se localizan en el mismo o en diversos planos, estos ductos van acomodados o insertados en el concreto de la losa y como están formados por diversos conductos son altamente resistentes a interferencias propiciadas por los servicios que por ellos mismos se distribuyen. Generalmente estos ductos son de acero de alta resistencia y la profundidad en el concreto, a la que son localizados varían de 25 mm a 1 cm.

El piso de acceso esta formado por paneles de piso modular soportados por pedestales con o sin seguros o encadenamientos laterales. Este es usado tanto en los cuartos de computadoras y de equipo, así como en el área general de oficinas. Donde el piso de acceso sea usado en áreas de oficina general, la altura mínima con respecto a la terminación del suelo debe ser 150mm, cuando es usado en los cuartos de equipo de telecomunicaciones esta altura mínima debe ser de 300mm y no menos de 150mm, para los closets de telecomunicaciones se emplea la misma altura que en las áreas de oficinas generales. El planteamiento para el piso de acceso debe ser determinado antes de la instalación de cualquier cableado o equipo de telecomunicaciones. Los closets de telecomunicaciones y el área de servicio de piso de acceso deben estar localizadas en forma adyacente una de la otra, conectadas mediante filamentos enchufados o conductos. El tamaño de las rutas de interconexión deben estar basadas en un criterio de diseño para un tipo de ruta específico.

Los tipos de conductores incluyen: tubo eléctro metálico y no metálico, conducto flexible no metálico y tubo flexible no metálico, conducto metálico rígido, conducto no metálico rígido y otros tipos. Los conductores los conductos deben ser de un tipo permitido por los propios códigos eléctricos. Si el conducto de metal flexible es usado, la longitud debe ser menor de 6m por cada corrida y el conductor seleccionado debe minimizar la abrasión del cable durante la instalación. Ninguna sección de conductos debe ser mayor de 30m ni contener más de dos curvaturas de 90° o equivalentes entre los puntos de enchufe.

Las cajas de salida no deben ser más pequeñas que 50 mm de ancho, 75 mm de altura y 64 mm de profundidad. Las cajas de enchufe deben ser usadas para los siguientes propósitos: fijar una corrida de conductor, la instalación de cadenas o cable.

Las charolas y wireways son estructuras rígidas prefabricadas para la protección y alojamiento de cables o conductores que son colocados después de que un sistema completo de rutas ha sido instalado. Las siguientes son ejemplos típicos de charolas y wireway para cables:

- Charola de canal para cables: estructura con una pieza ventilada o canal sólido cuya sección no excede 150mm de ancho.
- Charola de escalera para cable: estructura consistente de dos lados de rieles conectados individualmente en forma transversal.
- Charola sólida para cable: estructura consistente de una base sólida con rieles longitudinales.
- Charola ventilada para cable: estructura mayor a 100mm de ancho consistente de una parte ventilada con rieles de dos lados.
- Wireway: charola con bisagras o cubiertas removibles.

Las charolas o wireways deben estar divididas con separadores para la separación física de diferentes tipos del servicio como sea requerido. Deben estar localizadas abajo o arriba del techo o dentro del piso de acceso.

- **Rutas del backbone interno y espacios relacionados (Intrabulding backbone pathways and related spaces.**

Uno o más servicios de backbone pueden existir dentro de una construcción. Un servicio de backbone está generalmente formado por el "apilamiento" vertical de los closets de telecomunicaciones con pisos "abiertos" entre ellos. La unión de rutas también pueden existir para instalar el medio del backbone entre closets de telecomunicaciones en el mismo piso.

Las rutas del backbone pueden ser cualquier ruta de backbone interna horizontal o vertical extendida entre edificios. Las rutas de backbone interno están contenidas dentro de la construcción.

Las rutas de backbone interno típicamente consisten de rutas en techos, conductores, ranuras o cubiertas y charolas. Ellos proveen el significado de la localización de los cables de backbone entre el espacio o los cuartos de entrada, closets de telecomunicaciones, cuartos de equipo, o el espacio terminal principal. Las rutas verticales de backbone generalmente van desde el espacio principal

terminal hacia la pila vertical de closets de telecomunicaciones localizados en cada piso.

Estas rutas deben ser localizadas considerando los requerimientos de zonas sísmicas. Cuando se está considerando la instalación de rutas en zonas húmedas, las precauciones necesarias deben ser consideradas para que el agua no penetre en el sistema de ruteo.

- **Área de trabajo (Work area)**

Un área de trabajo es un espacio en la construcción donde los ocupantes normalmente interactúan con el equipo de telecomunicaciones. Los conectores de salida de telecomunicaciones en el área de trabajo son el punto en el cual el equipo de usuario final se conecta a la utilidad de telecomunicaciones de la construcción formada por la "ruta de espacio", y el sistema de cableado de la construcción.

Una salida de telecomunicaciones (caja o conector) es la localización del punto entre los cables horizontales y los cables de conexión de los dispositivos en el área de trabajo. Los dispositivos conectados son teléfonos, computadoras personales, y terminales de video y gráficas, cada una de las cuales requiere acceso al cableado de distribución horizontal mediante el conector de salida de telecomunicaciones.

Por lo menos una localización para la salida de telecomunicaciones debe ser instalado por área de trabajo. Para propósito de planeación, el espacio permitido por área de trabajo es aproximadamente $10m^2$.

La localización de las salidas de telecomunicaciones debe estar coordinado con la distribución del mobiliario. Una salida de potencia debe estar instalada cerca de cada caja de salida de telecomunicaciones. La localización de las salidas de telecomunicaciones es típicamente a la misma altura de la salida de potencia.

- **Closet de telecomunicaciones (Telecommunications closet)**

Un closet de telecomunicaciones es la facilidad de piso de servicio para el alojamiento del equipo de telecomunicaciones, terminadores de cable y lo relacionado con "cross-connections". El closet de telecomunicaciones es el punto de transición reconocido entre el backbone y las facilidades de rutas horizontales.

El closet de telecomunicaciones en cada piso es la localización reconocida de el punto de acceso para el backbone y las rutas horizontales. El closet de telecomunicaciones debe ser capaz de contener equipo de telecomunicaciones, terminaciones de cable y cable o cableado asociado al cross-connect. El closet de

telecomunicaciones debe estar localizado en el centro del área a servir. Las rutas horizontales deben terminar en el closet de telecomunicaciones localizado en el mismo piso así como las áreas a ser servidas. Las consideraciones de diseño a tomar en cuenta son:

- El espacio del closet de telecomunicaciones debe ser dedicado a las funciones de telecomunicaciones y soporte de las facilidades relacionadas. El espacio del closet de telecomunicaciones no debe ser compartido con instalaciones eléctricas y otras que no sean instalaciones de telecomunicaciones. Equipo no relacionado al soporte de telecomunicaciones (tuberías neumáticas, ductos hidráulicos, etc) no deben ser instalados en el paso, dentro o a través del closet de telecomunicaciones.
- Debe haber como mínimo un closet de telecomunicaciones por piso. Closets adicionales se deben considerar si: el área del piso a servir excede los 1000m^2
- La distancia de distribución horizontal hacia el área de trabajo es mayor a 90m.
- Varios closets en un mismo nivel deberán ser interconectados mediante un conducto que tenga un diámetro de 7.8 mm o una ruta equivalente.
- Los closets de telecomunicaciones deben dimensionarse de acuerdo a la tabla siguiente, en la cual se proporcionan las dimensiones mínimas aceptables de un closet de telecomunicaciones basadas en área de servicio no mayor a 1000m^2.

Área de Servicio	Tamaño del closet
1000 m^2	3 x 3.4 m
800 m^2	3 x 2.8 m
500 m^2	3 x 2.2 m

Tabla 3.7 Tamaño del closet de telecomunicaciones

- Los closets de telecomunicaciones deben estar localizados en áreas de piso diseñadas con una carga de piso mínima de 2.4 Kpa. Debe ser verificado que las concentraciones de equipo propuesto no excedan el límite de carga en el piso, estas especificaciones deben ser incrementadas para el caso de emplear equipo como mayor peso
- Deben existir en el closet de telecomunicaciones un mínimo de dos paredes con una cubierta rígida de A-C contramarchado a ¾ de pulgada y con una altura de 2.44 mm.
- La iluminación debe ser de 500 lx medidos a un metro arriba del piso, montados a 2.6 m mínimo sobre el piso raso.

- Para mayor flexibilidad, los techos falsos no deben considerarse para la construcción de closets de telecomunicaciones.
- Las puestas deben tener un mínimo de 91 cm de ancho y 2m de altura, debe abrir hacia fuera, ser removible o abrir de lado y debe tener cerradura.
- Las paredes pisos y techos deben ser tratadas para eliminar el polvo.
- Un mínimo de dos receptáculos de salida eléctrica ac duplex dedicadas de 120 v nominales, no conmutables, en cada circuito de Branco separada, deben ser provistas para el equipo de potencia. Estos receptáculos deben estar en el rango de 2A y ser conectadas hacia un circuito Branco de 20A. En suma, salidas duplex identificadas y marcadas convenientemente deben estar localizadas en intervalos de 1.8 m alrededor del perímetro d las paredes, con una altura de 150 mm arriba del suelo.
- El cuarto de telecomunicaciones debe situarse en un lugar de fácil acceso, considerando que no por eso se obstruirán sitios de tránsito normal, como podrían ser vestíbulos. Además sólo personal autorizado podrá acceder a los mismos.
- La protección contra incendios es requerida y debe ser prevista ya que es un código aplicable.
- Un sistema HVAC debe estar incluido en el cuarto de telecomunicaciones para mantener la misma temperatura en el área adyacente. Una presión positiva debe ser mantenida como mínimo de un cambio de aire por hora, o como sea requerido mediante un código aplicable. Cuando estén presentes dispositivos activos, un número suficiente de cambios de aire deben ser previstos para disipar el calor. Si está disponible una fuente de poder redundante en el edificio, el sistema HVAC que sirve al closet de telecomunicaciones, debe estar conectada a esta.

➢ **Cuarto de equipo (equipment rom)**

Un cuarto de equipo sirve a el espacio necesario para el equipo de telecomunicaciones más grande. Este es muchas veces un cuarto de propósito especial. Los cuarto de equipo están conectados a la facilidad de backbone. Este cuarto alberga solamente equipo relacionado directamente al sistema de telecomunicaciones y al sistema de soporte ambiental.

Los puntos a considerar para el diseño del closet de telecomunicaciones son:

- Se debe considerar la localización y distribución del closet de telecomunicaciones de acuerdo a los requerimientos de zonas sísmicas.
- Cuado se selecciona el sitio para el cuarto de equipo, evite localizaciones restringidas por componentes de la construcción que limiten la expansión como elevadores, fuera de las paredes, u otras paredes fijas construidas. El

- acceso a esta área debe ser restringido. Es deseable localizar el cuarto de equipo cerca de la senda del backbone.
- La capacidad del piso en el cuarto de equipo será suficiente para llevar la carga del equipo distribuido y el instalado. El cuarto de equipo se diseñará para una carga distribuida mínima de 4.8 KPa y un mínimo de carga de por lo menos 8.8 kN. Si extraordinariamente el peso del equipo es mayor estas características técnicas tienen que ser incrementadas.
- El cuarto de equipo no se localizará debajo del nivel de agua a menos que las medidas preventivas contra la infiltración de agua hayan sido empleadas. El cuarto está libre de agua o el desagüe que se conduce por tuberías no deberá estar localizado dentro del cuarto de equipo directamente.
- El cuarto de equipo se localizará con acceso listo al HVAC de entrega principal del sistema.
- El cuarto se localizará lejos de fuentes de interferencia electromagnética. Se prestará especial atención a los transformadores de suministro eléctrico, motores y generadores, equipo de la radiografía, radio o transmisores de radar y dispositivos de inducción.
- La vibración mecánica acoplada al equipo o a la infraestructura de cableado puede provocar fallas con el tiempo. Un ejemplo común de este tipo de fallas es la pérdida de conexiones.
- El tamaño del cuarto de equipo será determinado mediante el conocimiento de los requerimientos del equipo específico; esta información puede obtenerse del proveedor de equipo. Tomando en cuenta también proyectos futuros en los requerimientos presentes.
- Equipo del control ambiental, como distribuidores de potencia o sistemas de acondicionadores, y UPS arriba de 100 KVA se permitirán ser instalado en el cuarto de equipo. UPS más grande de 100 KVA que deben localizarse en un cuarto separado.
- Se verificarán esquemas con proveedores de equipo para el pero y limitaciones de distancia entre los armarios. Deben evitarse puertas que proporcionan acceso a otras áreas del edificio a través del cuarto de equipo para sólo limitar acceso al cuarto de equipo al personal autorizado.
- La altura mínima del cuarto será 2440 mm (8 ft) sin obstrucciones.
- El cuarto de equipo se conectará a la senda del backbone para el cableado hacia el espacio terminal principal y los closets de telecomunicaciones.
- Un HVAC deberá ser previsto las 24 hras del día, y los 365 días del año. Si el sistema del edificio no puede asegurar un funcionamiento continuo para aplicaciones de equipo grandes, una unidad independiente se mantendrá en el cuarto de equipo. Si una fuente de poder de reserva está disponible en el edificio, debe considerarse para ser conectada al sistema de HVAC para servir al cuarto de equipo de telecomunicaciones como suministro de reserva.

- Se sellarán suelo, paredes y techo para reducir el polvo. Los acabados serán en colores claros para reforzar la iluminación del cuarto. Se seleccionarán materiales que tengan propiedades antiestáticas.
- La iluminación debe ser de 500 lx medidos a un metro sobre el nivel del piso en medio de todos los pasillos entre los armarios. La iluminación será controlada por uno o más interruptores localizados cerca de la puerta de entrada al cuarto.
- Una fuente de suministro por separado que sirva a el cuarto de equipo se proporcionará y terminará en su propio tablero eléctrico.

➢ **Facilidades de entrada (Entrance facilities)**

Las facilidades de entrada consisten del servicio de entrada a la construcción, incluyendo la entrada a través de la pared del edificio, y continua hasta la entrada del cuarto o espacio de telecomunicaciones.

Las facilidades de entrada pueden contener las rutas del backbone que conectan el espacio terminal principal hacia otros edificios en situación de campo. Las especificaciones para las facilidades mencionadas deben cumplir con los requerimientos de zonas sísmicas. La localización de otras instalaciones como las eléctricas, agua y gas deben considerarse en la selección del lugar para localización de las facilidades de entrada de telecomunicaciones. Una facilidad de entrada alternativa debe ser prevista para prevenir necesidades especiales como seguridad, servicio continuo, etc. Equipo no relacionado al soporte de las facilidades de entrada. Las rutas que proveerán las facilidades de entrada pueden ser aéreas, "enterradas" , bajo tierra y en túneles.

Los siguientes elementos se consideran como parte de las facilidades de entrada:

- **Backbone entre edificios (Interbuilding backbone)**
  Facilidad de ruta hacia el cuarto de entrada o espacio provisto para la interconexión con otros edificios, como en un ambiente de campo.
- **Ruta de servicio de entrada (Service entrance pathway)**
  Facilidad de ruta hacia el cuarto de entrada o espacio previsto como la facilidad de entrada por el proveedor de servicios.
- **Punto de entrada (Entrance point)**
  Punto de emergencia del cableado de telecomunicaciones hacia el espacio en construcción.
- **Cuarto o espacio de entrada (Entrance room or espace)**
  Este espacio, preferentemente un cuarto, es la facilidad de servicio de la construcción en el cual la unión de las facilidades externas e internas toman lugar. El cuarto de servicio de entrada puede servir

también para cualquier función de telecomunicaciones para el equipo electrónico.

- **Entrada alterna (Alternate entrance)**
  Es una ruta para la duplicación o diversificación de los servicios de entrada y rutas entre construcciones.
- **Antenas de entrada (Antenna entrance)**
  Es una ruta hacia el cuarto de entrada asociado.

3.4.3 ANSI/TIA/EIA-606

Estándar para la Administración de la Infraestructura de Telecomunicaciones en Edificios Comerciales.

Las construcciones modernas requieren de una infraestructura de telecomunicaciones efectiva para soportar la amplia variedad de sistemas en los que confían la transportación electrónica de su información. Esta infraestructura abarca los espacios de equipos de telecomunicaciones, rutas de cableado, instalaciones de cableado de telecomunicaciones y hardware de terminación, aterrizaje de telecomunicaciones, y otros dispositivos. La administración de la infraestructura de telecomunicaciones incluye la documentación (etiquetas, esquemas, reportes, ordenes de trabajo, etc) de cableado, terminación de hardware de conexión, conductores, otras rutas de cableado, closets de telecomunicaciones y otros espacios de telecomunicaciones. La colección y periodo de actualización de la información es crítica para un proceso administrativo exitoso.

El propósito e intento de este estándar es proveer un esquema de administración uniforme que independiente de las aplicaciones, pueda cambiar varias a través de la vida del edificio. Dentro del control de los componentes de la infraestructura de telecomunicaciones se deberá asignar a cada componente un identificador único, para así tener identificador único, para así tener identificadores para cada ruta, espacio, cable, hardware y terminación, posición de terminación, empalme y componente de puesta a tierra (TMGB, TGB's conductores de unión, etc.). No sólo se deben asignar identificadores, sino que también se deben etiquetar los componentes de acuerdo a las siguientes reglas:

- Las rutas de cableado se deben etiquetar en cada terminación localizada en los closets de telecomunicaciones, cuartos de equipo o facilidades de entrada. Se recomienda si es posible etiquetar en localizaciones intermedias o en un espacio regular a lo largo de la ruta.
- Todos los espacios deben estar etiquetados. Se recomienda que las etiquetas se fijen en las entradas de los espacios.
- Los sub-sistemas de cableado horizontal y de backbone deben ser etiquetados en cada extremo. Se recomienda que se fijen etiquetas en cada extremo más que marcar el cable. Una etiqueta adicional al cable debe

estar localizada en una posición intermedia como son los extremos de conductos o empalmes, bocas de acceso y pull boxes.

- Se debe marcar un identificador en cada hardware de terminación.
- Un identificador debe ser marcado en cada etiqueta de posición de terminación. Cada posición de terminación debe ser marcada con el identificador de posición de terminación excepto en casos donde la alta densidad de terminaciones haga impráctica el proceso de etiquetado. Un identificador debe ser marcado en cada empalme o en su etiqueta.
- El buscar principal de unión de telecomunicaciones (TMGB) debe ser etiquetado con la marca "TMGB"
- Cada conductor del backbone y de unión de telecomunicaciones (TBB) conectado al TMGB debe ser marcado o etiquetado. Las etiquetas o marcas deben ser localizadas en los conductores y tan cerca como sea posible de la TMGB. Las etiquetas o marcas también serán colocadas en el otro extremo de este conductor de backbone de unión donde se enlazarán a los busbar de puesta a tierra de telecomunicaciones (TYGB's).
- Cada TGB deberá ser marcado o etiquetado.
- Es recomendable que todos los conductores de unión extendidos a los equipos desde cualquier TGB en el edificio sean etiquetados. Las etiquetas deben ser colocadas en los conductores tan cerca como sea práctico para el TGB.

Por concepto de administración, también se deben incluir registros de los componentes de acuerdo a las siguientes reglas:

- En los registros de ruta se debe incluir los identificadores de ruta, los tipos de ruta, el porcentaje de saturación de la ruta y la carga en la ruta. Adicionalmente, se deben mantener los enlaces a los registros de cables, registros de espacios (terminación 1), registro de espacios (terminación 2), registro de espacio (acceso), otros registros de ruta y registro de puesta a tierra.
- En cada registro de espacio se debe incluir el identificador de espacio y el tipo de espacio. Además de mantener los enlaces hacia registros de rutas, registros de cables y registros de puesta a tierra.
- Se debe registrar para cada cable: identificador de cable, tipo de cable, y los cables o conductores no terminados, dañados y disponibles. Además, debe contener enlaces a los registros de posición de terminación, registros de empalmes, registro de rutas y registro de puesta a tierra. El registro de cable debe documentar todo conductor en el cable. El campo de tipo de cable incluirá el fabricante y la descripción del fabricante. También será deseable el mes y año de la instalación o aceptación lo que será registrado en información opcional.
- Para cada elemento de hardware de terminación se debe de registrar su identificador de hardware de terminación, su tipo y posición. Además, se

deben registrar enlaces a los registros de posición de terminación, registros de espacios y registros de puesta a tierra.

- Se debe registrar de la posición de terminación su identificador, tipo, código de usuario y el número de pares/conductores. Además de contener enlaces a registros de cables, registros de posición de terminación, registro de hardware de terminación y registros de espacios.
- Para los empalmes se debe registrar el identificador de empalme y su tipo. Además debe contener los enlaces a registros de cables y registros de espacios.
- Para el TMGB se debe registrar el identificador "TMGB", el tipo de busbar, el identificador del conductor de puesta a tierra, la resistencia a tierra y la fecha que indica cuando fue tomada. Además debe contener ligas al registro de conductor de unión y al registro de espacio. Puesto que el edificio tiene solo un TMGB, un simple registro mantendrá toda la información relacionada al TMGB y al conductor de puesta a tierra del edificio.
- Para el backbone de unión se debe registrar en cada cable el identificador de conductor de unión, tipo de conductor e identificador de busbar (ya sea al TMGB o a algún TGB). Además se deben mantener ligas a registro de busbar y rutas.
- Para los TGBs, el registro debe contener identificador de buscar y tipo de busbar. Además de ligas hacia registros de conductor de unión y registros de espacios.

También se deben incluir dibujos con las siguientes especificaciones:

- Se debe mantener un dibujo de los elementos de la infraestructura del sistema de cableado. Este dibujo mostrará la localización de todas las terminaciones de cableado y de los cables de backbone. También se mostrará una ruta de todos los cables. El identificador de cada terminación y cable representado aparecerá en el dibujo.
- El dibujo del backbone mostrará vistas de planta y elevación de todos los cables de backbone que sean instalados y encaminados a través de las rutas de telecomunicaciones, closets, cuartos de equipo y facilidades de entrada.
- La localización de todos los empalmes será indicada.
- Se deben mantener dibujos que registren los elementos de la infraestructura de puesta a tierra. Estos dibujos mostrarán la localización del electrodo de puesta a tierra del edificio, la ruta del conductor del electrodo de puesta a tierra desde el electrodo de puesta a tierra al TMGB y todos los busbar de puesta a tierra conectados al backbone. Los dibujos también mostrarán la ruta de todos los conductores de puesta a tierra.

Las etiquetas a utilizar en los equipos, deben cumplir con los siguientes puntos:

- Las etiquetas de terminación que identifiquen el mismo cable deben ser del mismo color.
- Los cross-connection son generalmente implementados entre campos de terminación de dos diferentes colores.
- El color naranja (pantone 150C) identificará el punto de demarcación (terminación de la oficina central).
- El color verde (pantone 353C) debe ser utilizado para identificar la terminación de conexiones de red en el lado de servicio a usuarios del punto de demarcación.
- El color púrpura (pantone 264C) se usará para identificar la terminación de cables originarios de un equipo común (computadoras, PBX's, multiplexores, etc).
- El calor blanco será empleado para identificar el medio del primer nivel del backbone de telecomunicaciones en el edificio que contenga el cross-connect principal.
- El color gris (pantone 422C) debe ser utilizado para identificar el medio del segundo nivel del backbone de telecomunicaciones en el edificio que contenga el cross-connect principal.
- El color azul (pantone 291C) se usará para identificar la terminación del medio de la estación de telecomunicaciones y es requerido sólo en el extremo del closet de telecomunicaciones y es requerido sólo en el extremo del closet de telecomunicaciones (TC) y en el extremo de las facilidades de entrada (ER) del cable y no en el outlet connection de telecomunicaciones.
- El color café (pantone 465C) se utilizará para la identificación de las terminaciones del backbone entre edificios.
- El color amarillo (pantone 101C) se empleará para identificar la terminación de circuitos auxiliares (alarmas, mantenimientos, etc)
- El color rojo (pantone 184C) será empleado para identificar las terminaciones de sistemas telefónicos.
- En edificios que no contengan el cross-connect principal, el color blanco se utilizará para identificar las terminaciones del segundo nivel del backbone.

3.4.4 ANSI/TIA/EIA-607

Requerimientos de Unión Puesta a Tierra (aterrizaje) para Telecomunicaciones en Edificios Comerciales.

Las telecomunicaciones modernas requieren de una infraestructura efectiva dentro de su construcción para soportar la amplia variedad de sistemas en los que confían la transportación electrónica de su información. Esta infraestructura abarca los espacios de equipos de telecomunicaciones, rutas de cableado, instalaciones de cableado de telecomunicaciones y hardware de terminación, aterrizaje de

telecomunicaciones, y otros dispositivos. La infraestructura provee el soporto básico de la distribución de toda la información dentro del edificio. La unión de puesta a tierra recomendados en este estándar están propuestos para trabajar con la topología de cableado especificada en el ANSI/EIA/TIA-568-A (estándar de cableado de telecomunicaciones) e instaladas de acuerdo con el ANSI/EIA/TIA-569-A (estándar de rutas y espacios de telecomunicaciones).

El propósito de este estándar es hacer posible la planeación, diseño e instalación de sistemas de puesta a tierra de telecomunicaciones teniendo o no conocimiento previo de los sistemas de telecomunicaciones que subsecuentemente serán instalados. Esta infraestructura de telecomunicaciones de unión de puesta a tierra deberá soportar ambientes multiproductos y multiproveedores. En este estándar se especifican:

- Los requerimientos de unión de puesta a tierra de telecomunicaciones para una infraestructura uniforme que deberá ser seguida dentro de los edificios comerciales donde se intenta instalar los equipos de telecomunicaciones.
- La interconexión hacia otros sistemas de aterrizaje, soporte de sistemas y equipos de telecomunicaciones.
- El armazón o cuadro de unión puesta a tierra de telecomunicaciones.
- Una referencia de puesta a tierra de sistemas de telecomunicaciones dentro las facilidades de entradas de telecomunicaciones, los closets de telecomunicaciones y cuarto de equipo.
- La unión y rutas de conexión, protección de cables, conductores y hardware de closet de telecomunicaciones, cuartos de equipo y facilidades de entrada.

La infraestructura de unión de puesta a tierra de telecomunicaciones se origina con una conexión hacia tierra de los equipos de servicio (potencia) y se extiende a través de la construcción.

Este se conforma por 5 componentes principales:

- **Conductor de unión para telecomunicaciones**

El conductor de unión para telecomunicaciones debe unir al Busbar principal de puesta a tierra de telecomunicaciones (TMGB) hacia la puesta a tierra del equipo de servicio. La figura siguiente esquematiza esta conexión.

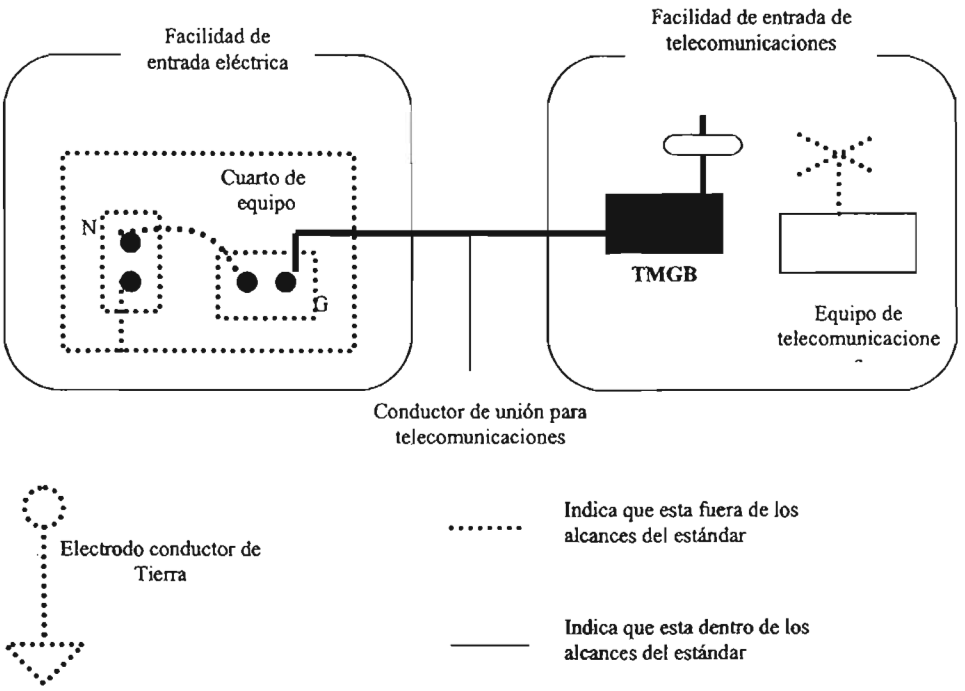


Figura 3.11 Esquema de conectividad hacia la tierra del equipo de servicio.

El conductor de unión para telecomunicaciones debe ser como mínimo del mismo tamaño que el TBB, es decir, 6 AWG.

- **Buscar (barra guía) principal de puesta a tierra de telecomunicaciones (TMGB)**

Se localizará en el cuarto de facilidades de entrada de telecomunicaciones del edificio y debe cumplir con:

- ❖ Ser una barra de cobre pre-perforado provisto con orificios para tornillos que cumplan con el estándar NEMA de tamaño y espaciado para el tipo de conectores que se empleen.
- ❖ Tener dimensiones mínimas de 6mm de grosor x 50 mm de ancho y variable en longitud para mantener los requerimientos de futuros aterrizajes.
- ❖ Ser galvanizado para reducir la resistencia por contacto.

Este TMGB se unirá al electrodo de tierra de las instalaciones de entrada eléctrica del edificio, y por otro lado se unirá al backbone de unión para telecomunicaciones (TBB).

➢ **Backbone de unión de telecomunicaciones (TBB)**

Un TBB es un conductor que interconecta todos los busbar de puesta a tierra de telecomunicaciones (TGB's) con el TMGB. La función básica de los TBB´s es reducir o igualar las diferencias de potencial entre los sistemas de telecomunicaciones unidos a este. Un TBB se origina en el TMGB, se extiende a través de la construcción usando las rutas del backbone de telecomunicaciones, y se conecta hacia todos los TGB´s en todos los closets y cuartos de equipos de telecomunicaciones.

El TBB debe ser diseñado tomando en cuenta el tipo de construcción, tamaño del edificio, requerimientos de telecomunicaciones y la configuración de las rutas y espacios de telecomunicaciones. El TBB debe ser un conductor de cable aislado y su tamaño mínimo debe ser de 6 AWG.

➢ **Busbar (barra guía) de puesta a tierra de telecomunicaciones (TGB)**

El busbar de puesta a tierra de telecomunicaciones es el punto central común de conexión para sistemas de telecomunicaciones y equipo localizado en el área de servicio mediante el closet de telecomunicaciones o cuarto de equipo. El TGB cumple con los puntos especificados anteriormente para el TGMB. El TGB deberá estar aislado de su soporte por una separación mínima de 50 mm y su localización ideal es al lado del panel de telecomunicaciones en caso de que exista en el closet o en el cuarto de equipo de telecomunicaiones.

➢ **Interconexión de unión del backbone de telecomunicaciones con el conductor de unión de puesta a tierra (TBBIBC)**

Estos componentes en conjunto con las rutas y espacios (ANSI/EIA/TIA-569) y el cableado de telecomunicaciones (ANSI/EIA/TIA-568), comprenden totalmente el soporte básico de una estructura de telecomunicaciones.

3.4.5. Estándares de Redes Inalámbricas.

Las transmisiones inalámbricas constituyen una potente herramienta de transferencia de información que permiten resolver varias de las restricciones derivadas de utilizar un punto de contacto en las redes locales convencionales. Se emplean para comunicar estaciones de trabajo a través de ondas de radio, permitiendo la movilidad y flexibilidad del sistema en general. Durante los primeros años de su existencia, estas redes estuvieron rodeadas por una serie de juicios, algunos ciertos y otros no, que contribuyeron, al menos parcialmente, a la lenta aceptación que han tenido.

La norma que rige las comunicaciones inalámbricas es la 802.11 Redes Inalámbricas (Gíreles LANs), que se convirtió en una norma aprobada por la IEEE en el año 1996, aunque han sido utilizadas tanto en la industria, en la oficina como en centros de investigación desde hace mas de 15 años. Son una herramienta de transferencia de información con una cobertura geográfica limitada, relativamente alta velocidad de transmisión, baja tasa de errores, administrada de forma privada y que utiliza el espectro, permitiendo acceder a beneficios tales como:

- **Flexibilidad**, ya que los cables sirven para unir las redes pero también pueden representar serias limitaciones cuando se requiere integrar o reubicar equipos para reorganizar oficinas, etc.
- **Ahorro de cableado**, al utilizar ondas de radio para su conexión, no es necesario el tener que invertir altas sumas de dinero en productos, instalación de cableado, racks y organizadores, conexiones, etc.
- **Movilidad**, las redes inalámbricas le permiten al usuario mantener la conexión hacia la red mientras deambulan por un edificio o algún campus con una computadora portátil.

Las redes inalámbricas sirven para evitar el uso de cables dentro de tuberías que no tienen espacio para un cable más, continuos experimentos para instalar, mover o mudar equipos en la oficina, desplazarse por la empresa sin perder el contacto con la red local, interconectar dispositivos a la intemperie, establecer reuniones "ad hoc" y grupos de trabajo de corto plazo, interconectar dispositivos en ambientes industriales con severas condiciones ambientales, interconectar redes locales entre dos edificios y como respaldo para reactivar partes críticas de una red en contingencias o siniestros. La figura 3.12 ejemplifica una configuración de una red inalámbrica.

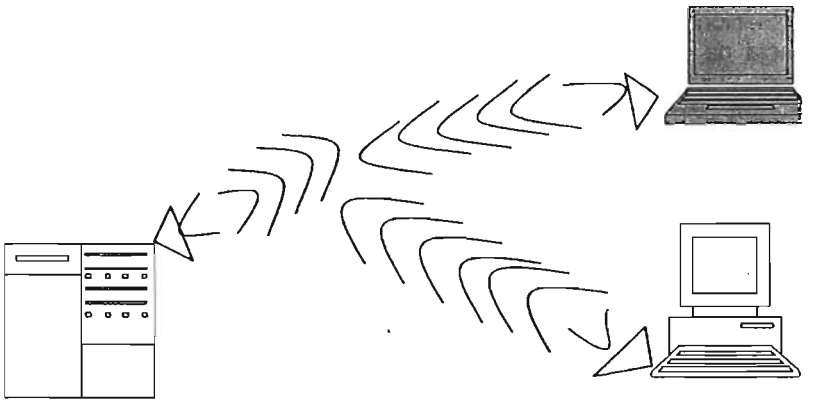


Figura 3.12 Redes Inalámbricas

Especificación 802.11

El comité 802.11 ha sido el desarrollador de las especificaciones para redes inalámbricas que soportan enlaces punto a punto y la infraestructura de redes inalámbricas locales vía punto de acceso a una red existente con sistema de cableado. Los protocolos desarrollados permiten al usuario móvil desplazarse con toda libertad por toda un área manteniendo la misma conexión, así como el poder de conversación. Además están disponibles dentro de pequeños dispositivos de computadoras móviles para comunicarse por largos periodos de tiempo con una sola carga de batería. A continuación se describen los puntos más importantes dentro del estándar 802.11 de Redes Inalámbricas.

Nivel Físico

A nivel físico el subcomité 802.11 menciona dos tipos de medios que se emplean con la LAN inalámbricas, las ondas de radiofrecuencia (R-F) y las señales ópticas de infrarrojo, siendo más utilizada la de radio por su mayor alcance aún entre objetos, pudiendo penetrar en paredes, pisos y el vidrio, lo que las hacen un medio más útil que los rayos infrarrojos en un entorno estructural más complejo, aunque los elementos infrarrojos tienen un precio más bajo que los de R-F y pueden transmitir a la misma velocidad que un enlace con cableado.

La Tecnología de Espectro Disperso fue desarrollada para evitar que las transmisiones de información militar y de inteligencia fueran interferidas y descifradas. Está diseñada para dar confiabilidad, integridad y seguridad, no

importando tanto el desempeño o velocidad de transmisión. El espectro disperso difiere de otras tecnologías de radio en que dispersa la señal transmitida sobre un amplia gama de frecuencias, utilizando un ancho de banda mucho mayor que el necesario por la velocidad de transmisión utilizada. Para ello mezcla la información transmitida con un patrón de dispersión que puede modificar la frecuencia o la fase (o ambas) de la información original, haciendo que esa sea extremadamente difícil de detectar por cualquier sistema que no tenga el mismo código de dispersión utilizado por el transmisor. Por otra parte, al distribuir la señal en una gama de frecuencias , se está también dispersando la potencia promedio transmitida, lo que es visto por otros dispositivos no acoplados con el transmisor, como una pequeña interferencia que peden descartar, permitiendo así que varios sistemas coexistan compartiendo las mismas frecuencias. Existen dos tipos o técnicas de modulación en espectro disperso operando en la banda de 2400-2483 MHZ:

- **Salto de Frecuencia (FHSS, Frequency Hopping Spread Spectrum)**
  Esta técnica de modulación divide la banda en muchos subcanales. La señal salta de subcanal a subcanal transmitiendo pequeñas ráfagas de datos en un canal por un periodo fijo de tiempo, llamado "dwell time". La secuencia de saltos debe estar sincronizada entre el transmisor y el receptor o la información se pierde. Comúnmente la banda se subdivide 75 subcanales y el "dwell time" no debe exceder 400ms. El salto en frecuencia es menos susceptible a interferencia porque la frecuencia cambia constantemente, además de ser más difícil de interceptar. Esto le da esta modulación una ventaja en el aspecto de seguridad de los datos. Para poder interceptar un sistema de este tipo es necesario "interceptar toda la banda"

- **Secuencia Directa (DSSS, Direct Sequence Spread Spectrum)**
  La secuencia directa, o seudo ruido, es la técnica mas empleada en los sistemas de redes inalámbricas. La modulación de secuencia directa ofrece un medio que garantiza la integridad y la seguridad de los datos. Los mensajes se rellenan con información de redundancia y corrección de errores. También es posible usar encriptación. Con la técnica de secuencia directa, los mensajes se codifican digitalizando cada bit, con un patrón multibit llamado "chip". Unos y ceros son representados por Chips que son inversores uno del otro. Cada bit cuando es transmitido, es propagado sobre un espectro de frecuencia amplia. El receptor colapsa cada chip transmitido dentro de un solo bit. Todas las señales que no son iguales son eliminadas, dando como resultado una señal libre de interferencias. Las transmisiones con secuencia directa tienen una relación señal a ruido mejorada con respecto a las transmisiones de banda estrella y se presentan mucho mejor para compartir el ancho de banda.

Los sistemas infrarrojos de corta apertura funcionan de manera similar a los controles remotos de los televisores: el emisor debe orientarse hacia el receptor antes de transferir información, lo que limita un tanto la funcionalidad. Los sistemas de gran apertura permiten la información en un ángulo mucho mas amplio por lo que el transmisor no tiene que estar alineado con el receptor.

La tecnología infrarroja cuenta con muchas características sumamente atractivas para utilizarse en la WLAN's: el infrarrojo tiene una longitud de onda muy cerca de la de la luz y se comporta como esta (no puede atravesar objetos sólidos); debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por dispositivos hechos por el hombre, en línea de vista se pueden alcanzar grandes velocidades de transmisión, de hecho, se han desarrollado sistemas que operan a 100Mbps. La transmisión infrarroja con láser o con diodos no requiere autorización especial en ningún país, utiliza componentes muy económicos y de bajo consumo de potencia, esencial para los dispositivos móviles (portátiles).

Entre las limitaciones principales que se encuentran en esta tecnología se pueden señalar las siguientes: es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre el emisor y el receptor, ya que requieren de una línea de vista limpia para la señal; las restricciones en la potencia de transmisión limitan la cobertura a redes a unas cuantas decenas de metros (aproximadamente 100 pies), la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.

A principios de 1994 la Asociación de datos por infrarrojo (Infrared Data Association) introdujo un estándar de codificación por medio de rayos infrarrojos. Este conjunto de especificaciones aseguraba que en 1995 existiría interoperabilidad entre productos basados en infrarrojos desarrollados para computadoras móviles. La tecnología de rayos infrarrojos se divide de la siguiente forma:

- **Línea de vista (Line of Sight)**
  La gran variedad de tecnología de infrarrojos con línea de vista está limitada a lugares como oficinas, donde no existan obstrucciones físicas para la señal entre las estaciones de usuarios. Aunque su naturaleza punto a punto restringe la distancia alrededor de 100 pies, la velocidad de transmisión puede igualarse a las redes basadas en el sistema de cableado que se encuentre en dicha instalación.

- **Infrarrojos por diseminación (Scatter Infrared)**
  La tecnología de redes locales por infrarrojos por diseminación rebota las señales en las paredes y techos para iluminar un área de aproximadamente

100 pies cuadrados. Esta característica produce una señal con una velocidad relativamente baja.

- **Rayos Infrarrojos reflejados (Reflective infrared)**
  En sistemas reflejados, los dispositivos de acoplamiento óptico (transceivers) son montados cerca de las estaciones o PC's y son dirigidos hacia un punto común sobre el techo de la oficina, esta propuesta trabaja bien en un ambiente con techos lisos.

Nivel de Enlace

Primero es necesario considerar los dos tipos de arquitectura de redes que especifica la norma:

- **Topología Ad-Hoc**
  Las estaciones se comunican directamente entre sí. No se requiere instalar infraestructura, estas redes son fáciles de operar pero su desventaja es un área de cobertura limitada. Estas estaciones forman un BSS (Basic Service Set, conjunto de servicio básico). La figura 3.13 muestra la configuración de la topología Ad-Hoc.

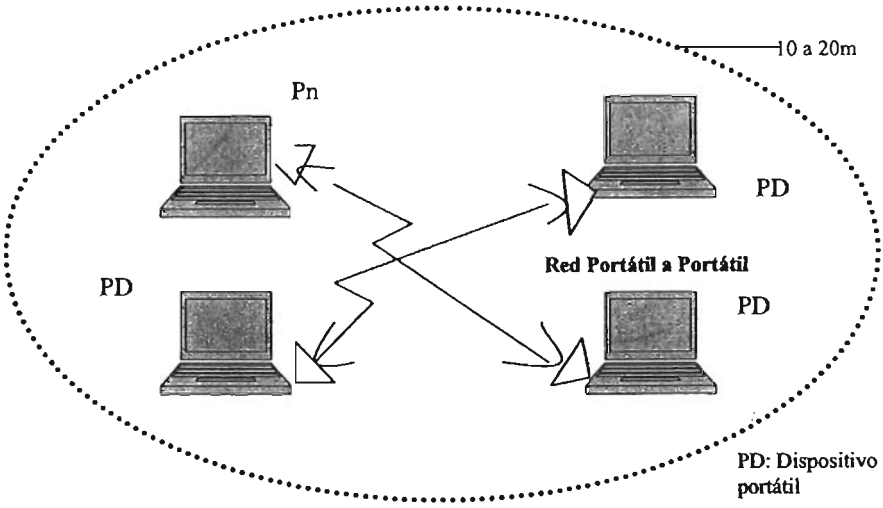


Figura 3.13 Topología Ad-Hoc

- Topología de Infraestructura

  Las estaciones se comunican a puntos de acceso (AP, Acces Point) que son parte del sistema de distribución. Un punto de acceso sirve a las estaciones en un conjunto de servicio básico o BSS. Todo el conjunto de BSS se llaman ESS (Extended Service Set, conjunto extendido de servicio). La norma sólo especifica la interfase inalámbrica, es decir, entre estaciones y, entre estaciones y puntos de acceso. Con un sistema de distribución, el área de cobertura se puede extender tanto como lo permitan las características del sistema. En la figura 3.14 se ejemplifica la topología de infraestructura.

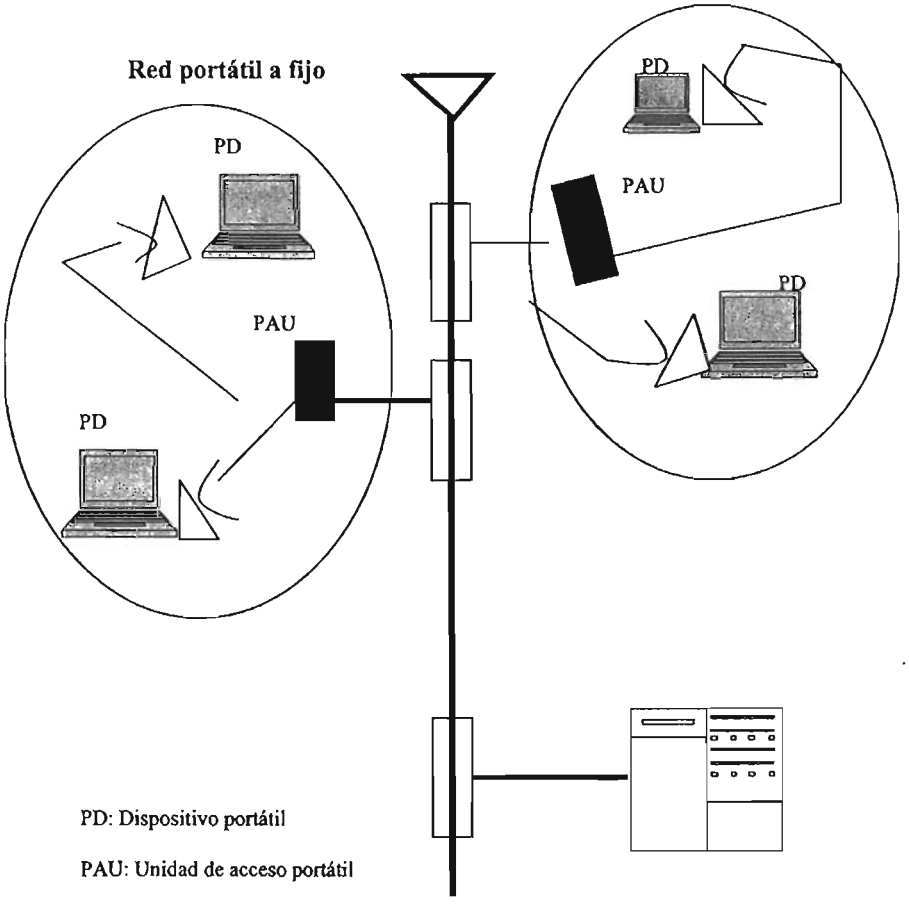


Figura 3.14 Topología en infraestructura

Como protocolo de acceso al medio, se sugiere que las redes inalámbricas empleen CSMA/CA (Carrier Sense Multiple Acces / Colision Avoidance). Este algoritmo evita colisiones, mientras que 802.3 sólo las detecta. El protocolo trabaja así: la estación "escucha" antes de transmitir, si alguien está transmitiendo, espera un tiempo aleatorio, entonces vuelve e intenta. Si nadie está transmitiendo, entonces manda un mensaje corto, este mensaje se llama RTS (Ready to Send, listo para enviar), este mensaje contiene la dirección destino y el tiempo de duración de la transmisión, por lo tanto, las otras estaciones ya saben cuanto tiempo va a estar ocupado el canal. El destino envía un mensaje corto llamado CTS (Clear to Send, libre para enviar), este mensaje le dice al destino que puede enviar información sin peligro de que existan colisiones. Cada paquete de datos requiere una confirmación a algún paquete, este lo reenvía. Esta secuencia es llamada "4-Way Handshake", la siguiente figura muestra el funcionamiento.

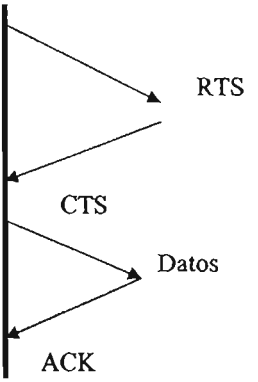


Figura 3.15 Secuencia "4-Way Handshake"

Framing 802.11 (Empaquetamiento)

El encabezado de la trama (frame) 802.11 consta de 7 campos con 30 bytes de largo. El campo de datos que puede ir de 0 hasta 2312 bytes y el campo de chequeo que es de 4 bytes.

Trama 802.11con longitud en bytes.

Frame control	Duration ID	Adress 1	Adress 2	Adress 3	Sequence 2	Adress 4	Frame Body	FCS
2	2	6	6	6	2	6	0-2312	4

Trama 802.11con longitud en bits.

Protocol version	Type	Subtype	To DS	From DS	More frag	Retry	Pwr Mgt	WEP	Order
2	2	4	1	1	1	1	1	1	1

CAPITULO 4. Dispositivos de Interconexión en Redes

4.1. Introducción

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (Internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de Interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta. Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (RAL con RAL)

  Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN)

- Interconexión de Área Extensa (RAL con MAN y RAL con WAN)

  La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN)

4.2. Repetidores

Los Repetidores son dispositivos activos de dos puertas para interconectar dos medios de comunicación con el objeto de amplificar y reformar los pulsos constituyentes de la señal. Usualmente se utilizan para extender la longitud de los cables en una LAN o conectar medios de tipo diferente, generando una LAN única más extensa.

Un repetidor interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI. Esto significa que los repetidores pueden sólo conectar LAN idénticas, tales como Ethernet/802.3 a Ethernet/802.3 o Token Ring a Token Ring, es decir; redes que tengan los mismos protocolos de nivel físico.

En el caso de una red de área local (LAN) o una red más amplia (WAN) el repetir paquetes resulta en una red, con un mejor performance, al regenerar los encabezados y resincronizar los 'data packet'.

Repetidores Token Ring, como los repetidores Ethernet, pueden usarse tanto para extender distancias como para conectar medios disímiles.

Los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Debido a esto existen más riesgos de colisión y más posibilidades de congestión de la red.

Se pueden clasificar en dos tipos:

- Locales: cuando enlazan redes próximas
- Remotos: cuando las redes están alejadas y se necesita un medio intermedio de comunicación.

4.2.1. Repetidores Ethernet

En el caso de una red Ethernet/802.3 los repetidores dejan pasar fragmentos en colisión tal de asegurar que todos los nodos respeten el sistema de detección de colisión. Un sistema de comunicación de datos puede contener múltiples segmentos de cable y múltiples repetidores. En una red Ethernet dos transceptores pueden estar separados hasta 2.5 km. (al usar fibra óptica) y ningún trayecto entre dos transceptores cualesquiera puede atravesar más de 4 repetidores.

Repetidores Ethernet/802.3 pueden tener sus 2 puertas idénticas o incluir combinaciones de los diferentes tipos permitidos por la norma IEEE 802.3. Por ello permiten interconectar segmentos diferentes. Por ejemplo 10Base5 a 10Base2 vía tranceptor , o 10Base2 a 10BaseT.

Cuando una colisión es detectada, el transceiver además coloca una señal especial en el cable (jam) para asegurar que todos los otros transceptores se percaten que ha ocurrido una colisión. El detector de jam cuenta el número de colisiones consecutivas. Sí esta cuenta excede un valor predefinido (e. g. 32), entonces el repetidor desactiva el segmento.

Sí se recibe un paquete válido desde ese segmento, el repetidor lo reactiva automáticamente. De esta forma, segmentos con problemas son desconectados y segmentos válidos reconectados en forma dinámica.

4.2.2. Puertas de Entrada/Salida Típicas de un Repetidor

a) Puerta Tipo AUI (Attachment Unit Interface)

Esta puerta consiste en un conector sub-D de 15 pines para la conexión de un Media Attachment Unit (MAU), el cual típicamente es un transceptor o un DTE (e. g. Una workstation). Utiliza un cable de 4 pares trenzados blindados más blindaje general con un largo máximo de 50 metros , 78 W típico, y un tiempo de propagación de 5.13 ns/m. La interfaz incluye pares balanceados para data in (par 1), data out (par 2), control in (par3), control out (par 4), blindaje para cada par, tierra general. Puede existir un quinto par para referencias de voltaje o alimentar el transceptor desde el computador.

b) Puerta Tipo 10 Base 2 (IEEE 802.3)

Esta puerta consiste en un conector BNC para la conexión a un segmento de cable coaxial delgado (Thin wire Ethernet). Este segmento permite la operación en banda base a 10 Mhz con un largo máximo de 185 metros y una cantidad máxima de 30 MAU, con espaciamiento mínimo de 0.5 metros.

4.2.3. Ventajas y desventajas de los Repetidores

Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que

limita la distancia máxima entre los nodos más lejanos de la red a 1.500 m. (enlazando con dos repetidores tres segmentos de máxima longitud, 500m.)

Ventajas:

- Incrementa la distancia cubierta por la RAL
- Retransmite los datos sin retardos.
- Es transparente a los niveles superiores al físico

Desventajas:

- Incremente la carga en los segmentos que interconecta.

La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), ThickEtehernet (10Base5), ThinEthernet (10Base2), TokenRing, Fibra óptica, etc.

4.3. Bridge (Puente)

Interconectan dos segmentos de red, entre niveles OSI 2 (DLL), permitiendo ampliar una LAN a límites que excedan los permitidos por la norma respectiva. Mientras que un repetidor deja pasar todo, incluyendo el ruido eléctrico, un bridge tiene la capacidad de almacenar, examinar y luego retransmitir solo aquel frame que necesita alcanzar el otro segmento, e.i. actúan como repetidores selectivos.

- Son útiles para aislar el tráfico entre dos redes del mismo tipo, disminuyendo el tráfico global en una red multi-LAN.
- Permiten también interconectar dos redes cuando estas difieren en el nivel OSI 2 (DLL) pero tienen el mismo nivel OSI 3 (network layer), e.g. una red Ethernet/802.3 y una red Token Bus utilizando el protocolo TCP/IP (ver Fig. 4.1.). En este caso el bridge debe dar el nuevo formato al paquete y preocuparse de la congestión (conexión de LAN rápida a LAN lenta).
- En este sentido dos redes conectadas mediante un bridge son dos redes físicamente separadas, pero lógicamente son una red única. Esto significa que las reglas de cableado se aplican a cada red individual, no a ambas, pero los niveles de red del protocolo pueden direccionar las redes puenteadas como si fueran una sola.

Las redes conectadas a través de bridge aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan

conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

Un bridge ejecuta tres tareas básicas:

- Aprendizaje de las direcciones de nodos en cada red.
- Filtrado de las tramas destinadas a la red local.
- Envío de las tramas destinadas a la red remota.

Se distinguen dos tipos de bridge:

- **Locales**: sirven para enlazar directamente dos redes físicamente cercanas.
- **Remotos o de área extensa**: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.

Se puede realizar otra división de los bridges en función de la técnica de filtrado y envío (bridging) que utilicen:

- **Spanning Tree Protocol Bridge o Transparent Protocol Bridge (Protocolo de Arbol en Expansión o Transparente, STP).** Estos bridges deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.
- **Source Routing Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor, SRP).** El emisor ha de indicar al bridge cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos TokenRing.
- **Source Routing Transparent Protocol Bridge (Bridge de Protocolo de Encaminamiento por Emisor Transparente, SRTP).** Este tipo de bridges pueden funcionar en cualquiera de las técnicas anteriores.

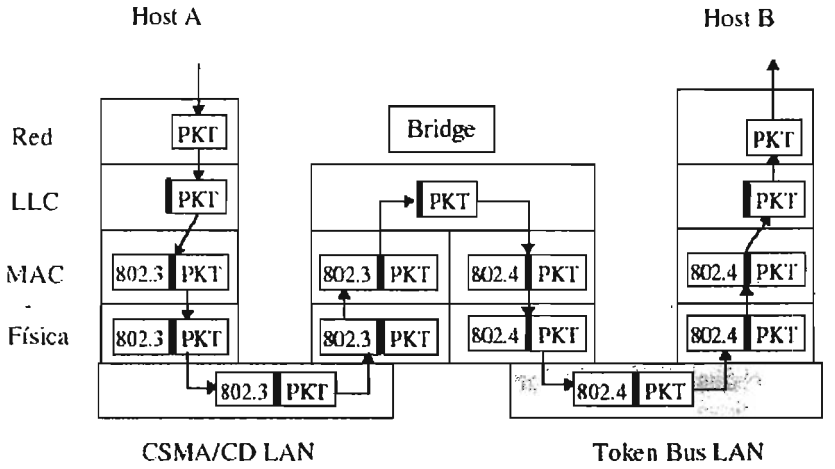


Figura 4.1. Funcionamiento de un bridge dentro de un modelo de capas.

4.3.1. Puentes Transparentes

Los puentes usados en LANs Ethernet 802.3 se llaman puentes transparentes. La razón es que los puentes son transparentes para las estaciones de trabajo, servidores de archivos, u otros dispositivos de redes. El puente realiza todas las funciones necesarias para encaminar el tráfico entre redes puenteadas. Puentes transparentes mantienen tablas de ruteo de la direcciones físicas de los dispositivos de la red y retransmiten tráfico basado en la ubicación (respecto al puente) de los dispositivos individuales de la red a los cuales es enviado el frame (Fig. 4.2).

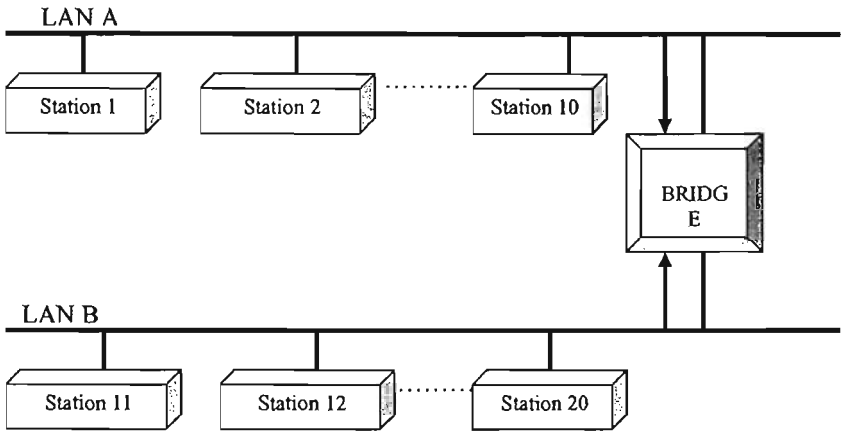


Fig. 4.2 Operación de un Bridge transparente.

Método de filtrado en un Puente Transparente

- El proceso comienza con la creación de una lista de direcciones de nodos locales enuna tabla llamada Source Address Table (SAT) mediante un proceso backward learning.
- Cuando el puente es conectado por primera vez, retransmite todo los paquetes que arriban a él. A medida que el puente recibe nuevos frames, almacena la dirección del remitente en la SAT junto con el segmento al cual pertenece dicha dirección.
- Si un remitente no envía paquetes en un lapso de 5 min. su dirección es borrada de la SAT. Esta característica se llama Aging Time. Este parámetro es programable en forma remota.

Para ilustrar el proceso de construcción de la SAT, consideremos la red de la figura 4.2. Cuando el nodo 1 envía un frame al nodo 20, el puente aprende la dirección de remitente del nodo 1 y la incorpora en la SAT indicando que pertenece al LAN A. Si a continuación el nodo 2 envía un frame al nodo 1, la dirección del nodo 1 será detectada en la SAT de la LAN A y el frame no será enviado a través del puente a la LAN B. Al mismo tiempo el puente aprenderá la dirección de remitente del nodo 2 agregándola a la SAT e indicando que pertenece a l LAN A.

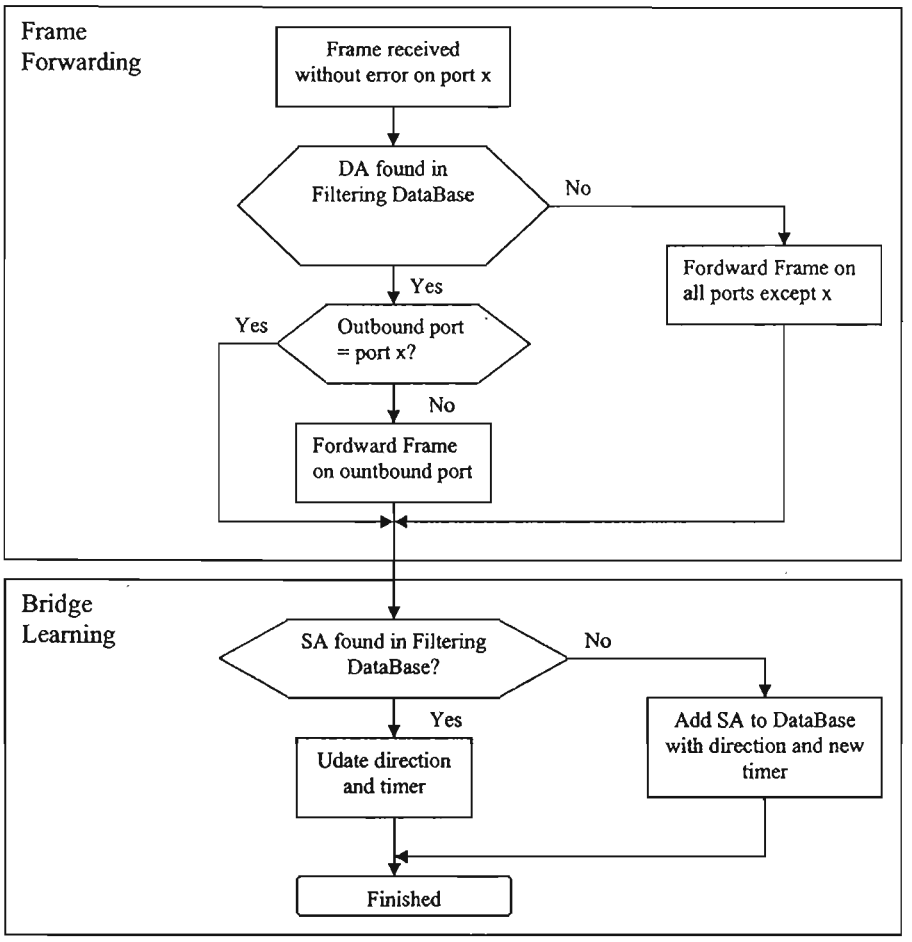


Fig. 4.3 Diagrama de aprendizaje y retransmisión de paquetes en un puente.

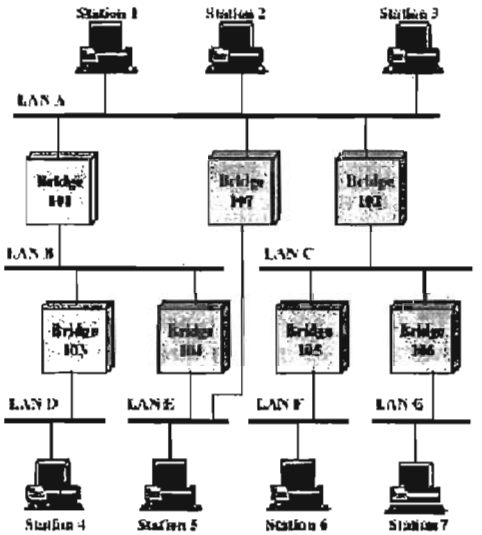


Fig. 4.4 Uso de puentes para interconexión de redes con rutas alternativas

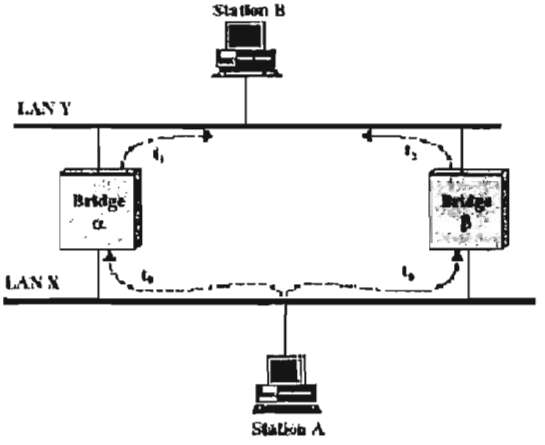


Fig. 4.5 Generación de lazos al interconectar redes a través de puentes

Spanning Tree Algorithm.

Los puentes transparentes en su esquema básico de operación no permiten la presencia decaminos redundantes, como el mostrado en la Fig. 4.4. Sin embargo, mediante el uso del algoritmo llamado Spanning Tree se permite trayectos alternativos y se elimina la presencia de lazos en la topología que produce el problema de la circulación indefinida de un paquete cuya dirección aun no esta en la tabla SAT en el lazo.

Por ejemplo en la Fig. 4.5, en el instante t_0 la estación A envía un paquete el cual pasará a la LAN Y a través de los puentes α y βen los instantes t_1 y t_2. Estos dos paquetes resultantes (F1 y F2) serán retransmitidos hacia la LAN X por los puentes β y α respectivamente ya que su dirección destino no existirá en las SAT (paquetes F3 y F4). Estos paquetes vuelven a ser retransmitidos a la LAN Y, y así sucesivamente.

Operación del algoritmo Spanning Tree:

- Se selecciona un puente raíz (Root Bridge), mediante un interruptor o comando SNMP. Este tiene ahora prioridad sobre todos los otros. Así se determina la trayectoria primaria en aquellas configuraciones de red que permiten lazos potenciales.
- Cada puente en un Spanning Tree debe aprender cual es el puente raíz y determinar su propia prioridad relativa dentro de la red.
- De este modo, esta jerarquía (o tree) de prioridades garantiza que los trayectos primarios y redundantes estarán claramente definidos en todo instante.
- Así solo un trayecto entre cualquier par de dispositivos está activo en un instante dado, el cual será el segmento de más bajo costo (e.i. el camino para la transmisión de datos que sea más económico para el nodo raíz).
- Los puentes redundantes son bloqueados en cuanto a transmisión de frames, pero continúan recibiendo información de topología de la red.
- Si un puente falla, otro puente (si existe) será activado automáticamente.
- La determinación del puente raíz comienza con la transmisión (broadcast) de Bridge Protocol Data Units (BPDUs), cuando este es encendido. Cada BPDU contiene un campo prioridad y su identificador único o dirección Ethernet.

4.3.2 Puentes con Ruteo en el Remitente (Source Routing Bridges)

A pesar de que puentes transparentes pueden usarse en redes Token Ring, IBM promociona otro método de puente llamado source routing, el cual a sido incluido en el estándar IEEE 802.5.

- Con esta técnica el puente no mantiene un control de la ruta por la cual son enviados los paquetes. Este control es realizado por nodo emisor.
- Para ello, durante la inicialización de la red, el nodo emisor envía discovery packets.
- Cada vez que un discovery packet llega a un puente este incluye su dirección (un número identificador único) en el paquete y lo transmite al siguiente LAN.
- El destinatario retorna su respuesta usando reverse addressing.
- La respuesta que llega más rápido corresponde a la ruta más económica.
- A continuación cada vez que el nodo emisor desee comunicarse, incluye en el frame la información de la ruta que seguirá el frame.
- Estos puentes permiten caminos redundantes.

4.3.3. Ventajas y desventajas de los Bridge

Ventajas de la utilización de bridges:

- **Fiabilidad.** Utilizando bridges se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- **Eficiencia**. Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- **Seguridad.** Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- **Dispersión.** Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los bridges permiten romper esa barrera de distancias.

Desventajas de los bridges:

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios bridges.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

Las aplicaciones de los bridges está en soluciones de interconexión de RALs similares dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento y transparencia a los protocolos de niveles superiores. También son útiles en conexiones que requieran funciones de filtrado. Cuando se quiera interconectar pequeñas redes.

4.4. Concentradores de Conmutación (Switches Ethernet).

Estos dispositivos corresponden a puentes multipuerta permitiendo reducir la cantidad de colisiones en una red Ethernet e incrementar el ancho de banda disponible para cada nodo. Esto se logra reduciendo el número de nodos por segmento lógico mediante técnicas de segmentación y switching de múltiples segmentos. Presentan la ventaja que esta operación se realiza con una latencia mucho menor a la de un puente básico (10 a 30 μs).

Estos dispositivos, debido a su bajo costo (US$ 100 a 200 por puerta en 1997), han empezado a reemplazar a los puentes y ruteadores como herramienta para incrementar el performance de una red Ethernet de 10 Mbps que presente deficientes tiempos de respuesta. Actualmente también existen switches que permiten mezclar redes Ethernet con Fast Ethernet (Switch departamental - switch backbone).

Basado en este dispositivo es posible crear redes Ethernet conmutadas que son la base de redes virtuales, esto es redes que pueden tener sus nodos geográficamente dispersos pero que constituyen una entidad única desde el punto de vista lógico o de direccionamiento.
Los concentradores de conmutación pasan los paquetes desde la puerta de entrada a la de salida a través de un conmutador de matriz de alta velocidad (~25 μs). Cuando un paquete llega a la puerta de entrada, se lee su dirección a nivel MAC (dirección Ethernet) y se encamina a la puerta donde está conectado el nodo de destino. Si la puerta está ocupada, el paquete se coloca en una cola (buffer de memoria en la puerta de entrada) hasta que la puerta de salida esté libre.

En un switch de acción directa (cut-through switching) está operación es realizada inmediatamente, extrayendo del encabezado del paquete sólo la dirección de destino (primeros 6 bytes). De esta forma, paquetes erróneos son igualmente retransmitidos y el nodo destino debe detectar los errores. Una variante mejorada de esta técnica es fragment-free cut-through la cual lee el

header completo (64 bytes). Así elimina la posibilidad que paquetes segmentados, producto de las colisiones (runts), se propaguen.

En un concentrador que utilice la técnica almacenar/reenviar (store and forward switching), el paquete entero es leído y analizado y los paquetes defectuosos o con errores rechazados. Esta acción introduce lógicamente una reducción de su velocidad.

4.4.1. Tipos de Swich

Hay tres tipos de conmutadores o técnicas de conmutación:

- Almacenar - Transmitir. Almacenan las tramas recibidas y una vez chequeadas se envían a su destinatario. La ventaja de este sistema es que previene del malgasto de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa ligeramente el tiempo de respuesta del switch.
- Cortar - Continuar. En este caso el envío de las tramas es inmediato una vez recibida la dirección de destino. Las ventajas y desventajas son cruzadas respecto a Almacenar -Transmitir. Este tipo de conmutadores es indicado para redes con poca latencia de errores.
- Híbridos. Este conmutador normalmente opera como Cortar -Continuar, pero constantemente monitoriza la frecuencia a la que tramas inválidas o dañadas son enviadas. Si este valor supera un umbral prefijado el conmutador se comporta como un Almacenar -Transmitir. Si desciende este nivel se pasa al modo inicial.

En caso de diferencia de velocidades entre las subredes interconectadas el conmutador necesariamente ha de operar como Almacenar -Transmitir. Esta tecnología permite una serie de facilidades tales como:

- Filtrado inteligente. Posibilidad de hacer filtrado de tráfico no sólo basándose en direcciones MAC, sino considerando parámetros adicionales, tales como el tipo de protocolo o la congestión de tráfico dentro del switch o en otros switches de la red.
- Soporte de redes virtuales. Posibilidad de crear grupos cerrados de usuarios, servidos por el mismo switch o por diferentes switches de la red, que constituyan dominios diferentes a efectos de difusión. De esta forma también se simplifican los procesos de movimientos y cambios, permitiendo a los usuarios ser ubicados o reubicados en red mediante software.

- Integración de routing. Inclusión de módulos que realizan función de los routers (encaminamiento), de tal forma que se puede realizar la conexión entre varias redes diferentes mediante propios switches.

4.5. Router (Enrutador)

Son dispositivos inteligentes que trabajan en el Nivel de Red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra. Convierten los paquetes de información de la red de área local, en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el encaminador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás routers para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre routers se realiza mediante protocolos de gestión propietarios.

Al igual que los puentes, los enrutadores pueden ser hardware propietario, o pueden ser un módulo de software residiendo en un computador de propósito general (e.g. un PC).

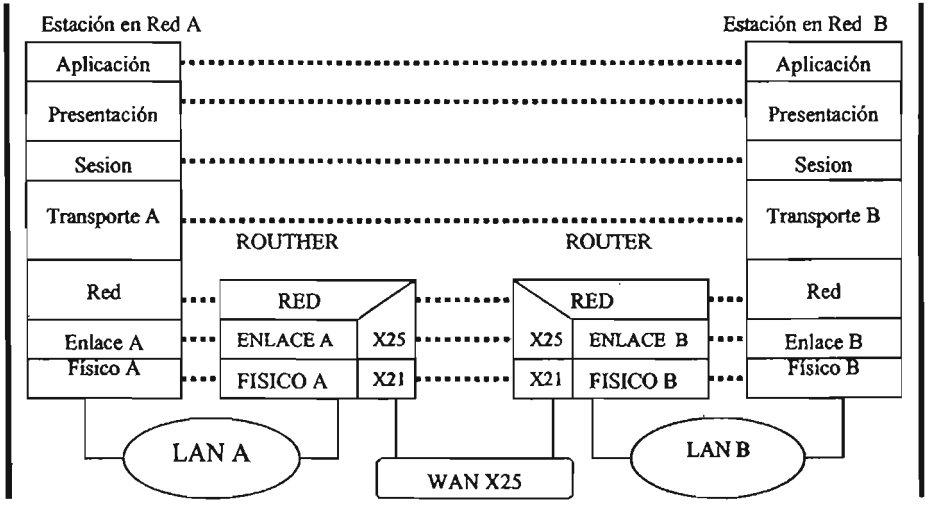


Fig. 4.6 Función de ruteo en el modelo ISO-OSI

4.5.1. Funciones básicas de los Routers

Permiten la interconexión de redes y subredes. Filtra y dirige el tráfico de la red interconectando los niveles OSI 3 de ambas redes (Network layer).

- Permiten conectar LANs que usan el mismo protocolo del Network layer (nivel 2), e.g. IP a IP pero con diferente sección de red en su dirección IP.
- Permiten conectar LANs que usan distinto protocolo del Network layer (nivel 2), e.g. IP a IPX esto es protocolo TCP/IP con Novel.
- Por el hecho de operar en el nivel OSI 3, los routers pueden también usarse para conectar redes con niveles 1 distintos, e.i. Arcnet, Ethernet, y Token Ring.
- Dos redes unidas por un router son dos redes separadas desde el punto de vista físico y lógico.
- Un router puede soportar uno o varios protocolos del nivel 3, e.g. IPX (red Novell), IP (red tipo Arpanet) y AppleTalk.

4.5.2. Clasificación de los Routers

Los encaminadores se pueden clasificar dependiendo de varios criterios:

- En función del área:
  - Locales: Sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al router.
  - De área extensa: Enlazan redes distantes.
- En función de la forma de actualizar las tablas de encaminamiento (routing):
  - Estáticos: La actualización de las tablas es manual.
  - Dinámicos: La actualización de las tablas las realiza el propio router automáticamente.

- En función de los protocolos que soportan:
  - IPX
  - TCP/IP
  - DECnet
  - AppleTalk
  - XNS
  - OSI
  - X.25

- En función del protocolo de encaminamiento que utilicen:

Routing Information Protocol (RIP)

Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de encaminamiento dinámicas y se intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

Exterior Gateway Protocol (EGP)

Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes routers para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

Open Shortest Path First Routing (OSPF)

Está diseñado para minimizar el tráfico de encaminamiento, permitiendo una total autentificación de los mensajes que se envían. Cada encaminador tiene una copia de la topología de la red y todas las copias son idénticas. Cada encaminador distribuye la información a su encaminador adyacente. Cada equipo construye un árbol de encaminamiento independientemente.

IS-IS

Encaminamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de encaminamiento en un dominio y entre diferentes dominios. Dentro de un mismo dominio el encaminamiento se realiza aplicando la técnica de menor coste. Entre diferentes dominios se consideran otros aspectos como puede ser la seguridad.

Otras variantes de los routers son:

- **Router Multiprotocolo**

Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los routers de segunda generación. No es necesario, por tanto, tener un router por cada protocolo de alto nivel existente en el conjunto de redes interconectadas. Esto

supone una reducción de gastos de equipamiento cuando son varios los protocolos en la red global.

- **Brouter (bridging router)**

Son routers multiprotocolo con facilidad de bridge. Funcionan como router para protocolos encaminables y, para aquellos que no lo son se comportan como bridge, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones. Operan tanto en el Nivel de Enlace como en el Nivel de Red del modelo de referencia OSI. Por ejemplo, un Brouter puede soportar protocolos de encaminamiento además de source routing y spanning tree bridging. El Brouter funciona como un router multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como bridge.

Las características y costes de los Brouter, hacen de estos la solución más apropiada para el problema de interconexión de redes complejas. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo, source routing y spanning tree e incluso de protocolos no encaminables. Son aconsejables en situaciones mixtas bridge/router. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo.

- **Trouter**

Es una combinación entre un router y servidor de terminales. Permite a pequeños grupos de trabajo la posibilidad de conectarse a RALs, WANs, modems, impresoras, y otros ordenadores sin tener que comprar un servidor de terminales y un router. El problema que presenta este dispositivo es que al integrar las funcionalidades de router y de servidor de terminales puede ocasionar una degradación en el tiempo de respuesta.

4.5.3. Ventajas y desventajas de los Routers

Ventajas de los routers:

- Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
- Flexibilidad. Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.

- Soporte de Protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- Relación Precio / Eficiencia. El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.
- Control de Flujo y Encaminamiento. Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas de los routers:

- Lentitud de proceso de paquetes respecto a los bridges.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los bridges.

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de RALs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

4.6. Gateway (Compuerta)

Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (Nivel de Transporte, Sesión, Presentación y Aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes.

Los gateways incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un bridge o un router, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos.

Los gateways tienen mayores capacidades que los routers y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y

permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

4.6.1. Tipos de Gateway

A continuación se describen algunos tipos de gateways:

- **Gateway asíncrono**. Sistema que permite a los usuarios de ordenadores personales acceder a grandes ordenadores (mainframes) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas conmutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.
- **Gateway SNA**. Permite la conexión a grandes ordenadores con arquitectura de comunicaciones SNA (System Network Architecture, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.
- **Gateway TCP/IP**. Estos gateways proporcionan servicios de comunicaciones con el exterior vía RAL o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.
- **Gateway PAD X.25**. Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.
- **Gateway FAX**. Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

4.6.2. Ventajas y desventajas de los Gateway

Ventajas:

- Simplifican la gestión de red.
- Permiten la conversión de protocolos.

Desventajas:

- Su gran capacidad se traduce en un alto precio de los equipos.
- La función de conversión de protocolos impone una sustancial sobrecarga en el gateway, la cual se traduce en un relativo bajo rendimiento. Debido a esto, un gateway puede ser un cuello de botella potencial si la red no está optimizada para mitigar esta posibilidad.

Su aplicación está en redes corporativas compuestas por un gran número de RALs de diferentes tipos.

4.7. Hub (Concentrador)

Un Hub permite derivar desde un segmento único varios segmentos del mismo u otro tipo, y así estructurar una LAN en mejor forma (ver Fig. 4.7). Los hubs pueden ser pasivos o activos. En los activos se incluyen las funciones básicas de un repetidor.

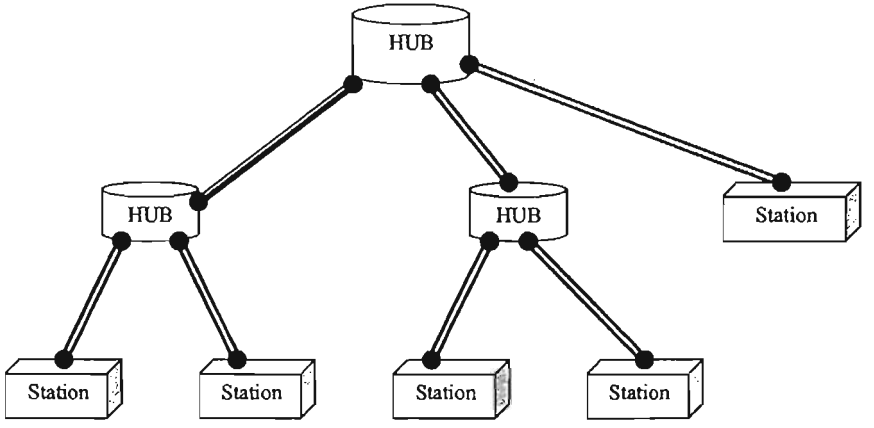


Fig. 4.7. Utilización de Hub de par trenzado para estructurar una LAN.

Para una red Ethernet - IEEE 802.3 los hub típicamente permiten:

- Hub 10Base2: derivaciones desde una red 10Base5 a múltiples segmentos 10Base2, para implementar conexiones multipunto.
- Hub 10BaseT: derivaciones desde una red 10Base2 a múltiples segmentos 10BaseT (Fig. 4.7). Los concentradores 10BaseT son realmente repetidores multipuerta.
- Usualmente la entrada al Hub es con cable AUI proveniente de un transceptor pasivo.

El término concentrador o hub describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Se suele aplicar a concentradores Ethernet, Token Ring, y FDDI(Fiber Distributed Data Interface) soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y TokenRing).

4.7.1. Evolución de los Hubs

Los primeros hubs o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica), y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.

Los hubs inteligentes de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un período mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.

Los nuevos hubs de "tercera generación" ofrecen proceso basado en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, TokenRing, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

A un hub Ethernet se le denomina "repetidor multipuerta". El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del hub. En el otro extremo de cada cable está un nodo de la red, por ejemplo un ordenador personal. Un hub Ethernet se convierte en un hub inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control.

Los concentradores inteligentes (smart hub) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. La capacidad de gestión remota de los hubs inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la RAL, con lo que otros usuarios no se ven afectados.

El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

A un hub TokenRing se le denomina Unidad de Acceso Multiestación (MAU) Multiestation Access Unit). Las MAUs se diferencian de los hubs Ethernet porque las primeras repiten la señal de datos únicamente a la siguiente estación en el anillo y no a todos los nodos conectados a ella como hace un hub Ethernet. Las MAUs pasivas no tienen inteligencia, son simplemente retransmisores. Las MAUs activas no sólo repiten la señal, además la amplifican y regeneran. Las MAUs inteligentes detectan errores y activan procedimientos para recuperarse de ellos.

4.8. Segmentación con conmutadores y enrutadores

Los switches entregan un alto throuput con baja latencia, pero tienen sus desventajas:

- Cualquiera red plana está sujeta a tormentas de broadcast, lazos spanning tree y limitaciones en las direcciones IP. Por ello, se hizo común a fines de los años80 de ruteadores en redes que incorporaban bridges.

Por ello, a comienzos de los años 90, debido al continuo nivel de integración y disminución de costo de circuitos ASIC, aparecen en el mercado switches que incluyen adicionalmente la función de ruteo.

Inicialmente, la función de ruteo es incorporada como un módulo software ejecutado mediante un microprocesador RISC que opera en paralelo con el ASIC que implementa la función de switching.

Posteriormente, la función de conmutación y ruteo IP es ejecutado en un único ASIC de alta velocidad, permitiendo muy altos velocidades de ruteo en el orden de 1 a 10 Megapackets/sec (1998).

Estos dispositivos se utilizan principalmente al estructurar una red con una arquitectura de backbone colapsado.

Tipos de Switch/Routers

Los fabricantes en su afán de aparecer introduciendo una nueva tecnología le han asignado a sus técnicas diversos nombres:

ASCI-assisted routing, zero hop routing, IP Switching, NetFlow, tag switching, Fast IP, multiprotocol over ATM (MPOA) routing, route servers, etc.

Pero todas estas técnicas se pueden reducir a dos grandes clases:

packet-by-packet and cut-through.

1) **Packet-by-packet layer 3 switches.**

Estos dispositivos al igual que los ruteadores convencionales, examinan cada paquete y luego lo reenvían a sus destinos. Ejecutan protocolos tal como OSPF, incorporan memorias cache para las tablas re ruteo y mantienen información de la topología de la red LAN. Por ello, funcionalmente tienen muy poca diferencia con un ruteador convencional. La gran diferencia surge en la razón precio/performance: Mpps por menos de US$ 20.000

2) Cut-through layer 3 switches.

Estos dispositivos analizan el primer paquete o serie de paquetes para determinar el destino. Una vez conocido el destino, se establece una conexión y el flujo de paquetes es conmutado en la capa 2, permitiendo los bajos delays y altos throughputs inherentes a un switch de la capa 2.

Pros y Contras

- Ambas técnicas proveen los beneficios de un alto throughput de una red plana sin los riesgos de broadcast y seguridad.
- Conocido vs nuevo. Packet-by-packet layer-3 switches implementan una solución conocida para interconectar redes, comparada con la nueva técnica cut-through que es más complicada a pesar de ser de arquitectura más limpia y elegante.
- Performance. La técnica packet-by-packet sufre en forma inherente de una latencia mayor. Sin embargo, los switches cut-through pueden perder velocidad debido a la inicialización de la conexión o limitaciones en la técnica de retransmisión en el nivel 2.
- Distribuido vs. Centralizado. El modelo packet-by-packet es distribuido, lo cual significa multiples switches layer-3 en una LAN grande (e.i. mayor costo de equipamiento y soporte). En cambio, el modelo centralizado de ruteo cut-through puede llegar a ser un cuello de botella o un punto único de falla.
- Interoperabilidad vs. Solución propietaria. Actualmente la tecnología cut-through se encuentra entre estándares a "medio cocinar" e invenciones propietarias casi-abiertas, resultando en una escasa interoperabilidad. Los switches layer-3 pueden interactuar con cualquier ruteador en la red o con switches de otros vendedores.

4.9. Tendencias Tecnológicas y de mercado

Las principales tendencias del mercado de sistemas de interconexión de redes son las siguientes:

- Tendencias de encaminamiento

El mercado está en expansión, cada vez hay más ofertas de productos y además estos incorporan nuevas facilidades de encaminamiento. Tanto los fabricantes de concentradores como los de multiplexores están incorporando en sus productos capacidades de encaminamiento, unos con redes de área metropolitana y extensa, y otros incorporando facilidades de interconexión de RALs.

- Equipos de interconexión a bajo coste

Los fabricantes están presentando equipos de bajo coste que permiten la interconexión de dependencias remotas. Las soluciones de encaminamiento son de diversos tipos: integradas en servidores de red, en concentradores, en pequeños equipos router, etc. Todos estos productos son fáciles de gestionar, operar y mantener.

- Routers multiprotocolo

Estos dispositivos han permitido a los usuarios transportar protocolos diferentes sobre la misma infraestructura de red, lo cual permitiría ahorrar en costes de la infraestructura de transmisión y una potencial mejora de la interoperabilidad.

- Interconexión de LAN/WAN bajo Switchers

Los conmutadores han evolucionado rápidamente dotándose de altas capacidades y velocidad de proceso. Pensados para soportar conmutación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) bajo una arquitectura punto a punto, han logrado gran implantación como mecanismo de interconexión de redes de área local heterogéneas, Token Ring y Ethernet en un mismo dominio. Esto se consigue dado que el conmutador permite la segmentación de la red en subredes conectadas a cada uno de sus puertos que puede gestionar de manera independiente.

- Capacidad de gestión

Los fabricantes están dotando a sus dispositivos de interconexión con mayores capacidades de gestión que permitan la monitorización de la red mediante estaciones de gestión y control de los dispositivos de la red, enviando comandos por la red desde la estación de gestión hasta el dispositivo de la red para cambiar/inicializar su configuración.

4.10. Descripción y comparación de Redes LAN Rápidas

En una red de área local (LAN), para cualquier usuario típico (e.i. que no utiliza aplicaciones de video o imágenes) una velocidad de conexión a la red de 10Mbps era y es suficiente. Por ello, a este nivel redes Ethernet y Token Ring son alternativas válidas. Pero con la aparición de nuevas aplicaciones (CAD/CAM, trasferencia de imágenes, etc.), de Intranets con servidores Web, o de servidores de bases de datos, esta velocidad ya no es suficiente para proveer la conectividad a grupos de servidores o la interconexión de grupos de trabajo a través de un backbone. Estos factores han generado la necesidad de incorporar en cualquier red institucional redes de alta velocidad, esto es con velocidades iguales o mayores a 100 Mbps.

En la actualidad, en aplicaciones para sistemas administrativos o comerciales, existen básicamente cinco ofertas tecnológicas en el campo de LAN con velocidades del orden de 100 Mbps. Entre estas tecnologías, Ethernet tiene la preeminencia del mercado. En 1996, más del 83% de las conexiones de redes LAN eran Ethernet o Fast Ethernet. Esto representa sobre 120 millones de PCs, estaciones de trabajo y servidores interconectados. El resto de las conexiones de redes rápidas son alguna combinación de Token Ring, 100-VG-Anylan, Fiber Distributed Data Interface (FDDI) o Asynchronous Transfer Mode (ATM).

Como muestra la Tabla 4.1, la razón entre despachos Ethernet y ATM era de 255 a 1. Se prevé que esta diferencia no se reducirá significativamente en los próximos 5 años.

	Hubs+Switches ports (miles)	Network Interf. (miles)	% del total
Ethernet (10 y 100 Mbps)	62.151	33.507	89.71
Token Ring	5.823	3.996	9.21
FDDI	580	149	0.68
ATM (all speeds)	316	110	0.40

Tabla 4.1. Entregas mundiales de redes LAN en 1996

De estas tecnologías, Token Ring actualmente provee sólo 4 y 16 Mbps y la versión HSTR (High Speed Token Ring) a 100 Mbps ha sido sólo recientemente propuesta por IBM a los organismos de estandarización, esperándose los primeros productos a mediados del 98. Por estas razones no será considerada en este análisis.

Las redes 100VG-AnyLAN tampoco serán consideradas por la baja aceptación que han tenido en el mercado pese a proveer una técnica de acceso al medio ligeramente superior al CSMA/CD de Ethernet.

Para velocidades mayores a 100 Mbps hay actualmente sólo dos tecnologías: ATM y Gigabit Ethernet.

Luego, las 4 arquitecturas de redes LAN rápidas que serán descritas y luego evaluadas son:

- Fast Ethernet
- FDDI
- ATM
- Gigabit Ethernet

4.10.1. Descripción de tecnologías LAN rápidas

4.10.1.1. FDDI

- FDDI transmite a velocidades de 100 Mbps sobre cable UTP categoría 5 (100 m entre repetidores), fibra óptica multimodo (2 km entre repetidores) y unimodo.
- Como método de acceso al medio utiliza token passing. Esta característica permite una baja degradación de performance con aumentos del tráfico (esto es, utiliza hasta 90% del ancho de banda).
- Utiliza una topología tipo anillo, ya sea anillo simple o doble. En la arquitectura de anillo doble, normalmente un anillo está activo, y cuando el anillo primario falla, el segundo entra en servicio gracias al protocolo SMT. La implementación de un anillo doble la hace altamente tolerante a fallas.
- FDDI permite transmitir frames de hasta 4500 bytes, permitiendo un throughput más alto que otras tecnologías que operan a la misma velocidad.
- Todas estas ventajas son contrapesados por un más alto costo (600 a 800% mayor que Fast Ethernet), lo cual la justifica sólo cuando se

- requieren conexiones a 100 Mbps con un alto grado de confiabilidad intrínseca respecto a daños del medio físico.
- Los datos pueden ser conmutados y ruteados hacia o desde una red Ethernet o Fast Ethernet sólo una vez que el formato y largo del frame son traducidos.

4.10.1.2. Fast Ethernet

- Fast Ethernet o 100BasetT (IEEE 802.3u) permite transmisiones a 100 Mbps sobre cable UTP categoría 5 y fibra óptica unimodo y multimodo.
- Al igual que la arquitectura Ethernet de 10 Mbps, Fast Ethernet (FE) utiliza la técnica de acceso a medios compartidos llamada CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Por ello, en medios compartidos, las colisiones resultantes hacen que FE pueda proveer tasas de transferencia de información sólo de 30 a 40%, con burst limitados de 90%, del ancho de banda del canal.
- FE utiliza el mismo formato y largo de frame que Ethernet (1518 bytes), por lo cual no requiere cambios en los protocolos de capas superiores, aplicaciones y software de redes para que sean ejecutados en computadores pertenecientes a una red de área local (LAN) que evoluciona desde esta popular tecnología.
- En el caso de FE conmutado (switched Fast Ethernet), una nueva característica es la opción de utilizar la capacidad fullduplex del medio, eliminando las colisiones y limitaciones topológicas (e.g. el largo del dominio de colisiones). La operación fullduplex puede ser configurada manualmente o mediante auto configuración. De esta forma, FE provee el doble de ancho de banda que FDDI (i.e. 200 Mbps), con comunicación bidireccional simultánea a una distancia máxima de 2 Km utilizando fibra óptica multimodo. Utilizando FE conmutado se tiene el perfil de performance (sin colisiones ni degradación) y características de redundancia necesarias para ser aplicada en backbones.
- Las dos mayores ventajas de FE respecto a FDDI es su costo más bajo y su fácil integración a la arquitectura Ethernet tradicional. Sus características de autonegociación y autosensing de la velocidad de comunicación facilitan esta tarea. Por ello su aplicación está aumentado rápidamente en conectividad de sistemas cliente servidor.

4.10.1.3. Asynchronous Transfer Mode (ATM) y ATM LAN Emulation

- ATM es una tecnología de multiplexing y conmutación orientada a la conexión, que utiliza celdas de 53 bytes (5 bytes de header, 48 bytes de data). El tamaño de las celdas utilizadas la adecua a la transmisión simultánea de voz, video y datos.
- Existen a lo menos cuatro alternativas para la aplicación de Raw ATM a redes de datos: LAN encapsulation in ATM (RFC 1483), Classical IP over ATM (RFC 1577, Jan. 1994), ATM LAN emulation (LANE) versión 1.0 y 2.0 (1995 y 1996), y Multi Protocol over ATM (MPOA).
- El uso de Classical IP over ATM exige que ambos dispositivos soporten el estándar ATM tanto a nivel físico como del protocolo en los niveles superiores. Classical IP se utiliza fundamentalmente en la interconexión de redes locales para formar una WAN o en el backbone de redes LAN, donde el tráfico es solamente IP. Esta característica permite ejecutar los protocolos del nivel de transporte TCP y UDP y aplicaciones tales como WWW, FTP, NFS, directamente sobre ATM.
- Al utilizar Classical IP con circuitos virtuales ATM permanentes (PVC), las direcciones IP deben asociarse manualmente a las direcciones ATM. Si los circuitos virtuales son conmutados, debe incluirse un servidor ATMARP (ATM Address Resolution Protocol).
- ATM LAN emulation consiste en un servicio Raw ATM mas una capa de adaptación a los estándares de capa MAC (Media Access Control) ya establecidos en redes locales (e.g. Ethernet o Token Ring). De esta forma se puede utilizar todos los drivers y adaptadores de estos estándares establecidos, generándose la interoperabilidad entre backbones ATM y grupos de trabajo operando con tecnologías de menor velocidad.
- La configuración típica donde es aplicable LANE es una LAN con Ethernet (o Fast Ethernet) operando con un backbone ATM. En este caso el protocolo sobre Ethernet probablemente será TCP/IP. Cuando no se defina una red desde cero sino que ya existen redes no ATM operando, la mejor alternativa para incorporar ATM será LANE o MPOA.
- Las dos velocidades actualmente más utilizadas son 155.52 Mbps (OC-3) y 622.08 Mbps (OC-12), y el nivel físico está determinado por el estándar SONET/SDH.
- Una de las grandes ventajas de ATM es que provee servicios de asignación dinámica del ancho de banda total para cada uno de los usuarios que comparten el canal físico, creando canales y pasos virtuales.
- Raw ATM ofrece varias clases de servicio. Servicio Clase C (variable bit rate, asynchronous) es el que se adecua al trafico típico de una LAN. Por ello el protocolo de la ATM Adaptation Layer (AAL) es el tipo ¾ (bit rate variable).

- ATM ofrece tres tipos de transmisión:
  - Full duplex a 155.54 Mbps en cada dirección
  - Subscriptor a red a 155.54 Mbps y red a subscriptor a 622.08 Mbps
  - Full duplex a 622.08 Mbps

	Medio	Dis. Máx.	Estándar	Código
Full duplex 155.54 Mbps	Coaxial (dos)	100 a200 m	G.703	CMI
	Fibra Óptica Single modo	800 a 2000 m	G.652	NRZ
Half o Full duplex 622 Mbps	Fibra Óptica Single modo	800 a 2000 m	G.652	NRZ

Tabla 4.2. Características de Redes ATM.

4.10.1.4. Gigabit Ethernet (IEEE 802.3z)

- Basada en la casi aceptación universal de la tecnología Ethernet 10Base-T operando a 10 Mbps, la tecnología Fast Ethernet ha provisto una evolución suave y no disruptiva hacia el performance de 100Mbps. Análogamente, Gigabit Ethernet provee un ancho de banda de 1 Gbps para redes de campus con la simplicidad de Ethernet a un costo más bajo que otras tecnologías de velocidades similares.
- Gigabit Ethernet usa el mismo protocolo (CSMA/CD), el mismo formato y tamaño de frame que sus predecesores operando a 10 y 100 Mbps. Además, también soporta operación half-duplex (en segmentos compartidos o shared) y full-duplex, permitiendo en esta segunda modalidad la implementación de backbones conmutados operando a 2 Gbps.
- Dos nuevas características han sido agregadas a CSMA/CD para permitir una operación eficiente halfduplex en el diámetro práctico del dominio de colisiones resultante de la velocidad de 1000 Mbps. Estas dos características que solo afectan al modo de operación half-duplex son : carrier extension y packet bursting. Carrier extension permite adaptar paquetes de menos de 512 bytes, a dicho largo mínimo tal que las colisiones sean detectables en la extensión total del segmento. Packet bursting permite a los dispositivos enviar grupos de paquetes pequeños de forrma tal de maximizar la utilización del ancho de banda.
- En el modo full-duplex, la operación es idéntica a Fast Ethernet, sólo más rápida. Esto es, los dispositivos continúan utilizando el interframe gap de 96 bits y largo mínimo de paquete de 64 bytes. La operación full-duplex es posible sobre la longitud máxima del enlace especificada para cada medio físico de transmisión.
- Un nuevo dispositivo es introducido, llamado buffered distributor o fullduplex repeater. Este es un dispositivo fullduplex, multipuerta, similar a

- un hub el cual interconecta 2 o más enlaces 802.3 operando a 1 Gbps o más rápido. Al igual que el repetidor 802.3, es un dispositivo que no filtra direcciones, sino que envía todos los paquetes que arriban a todos los enlaces conectados excepto el enlace de origen, proveyendo de esta forma un dominio de ancho de banda compartido comparable al dominio de colisiones de 802.3. A diferencia del repetidor 802.3, el distribuidor con buffer puede acumular uno o más frames arribados por cada enlace antes de reenviarlos. Además incorpora control de flujo implementando el estándar IEEE802.3x, lo cual elimina la posibilidad de pérdida de frames por rebalse del buffer.
- De este modo, Gigabit Ethernet ofrece el modo de operación fullduplex no sólo en switches sino que también en Hubs. Así un hub Gigabit Ethernet operando en el modo de repetidor fullduplex (i.e. sin colisiones) puede alcanzar un tasa de transferencia de hasta 95% del ancho de banda disponible (i.e. 1Gbps aproximadamente en cada dirección), aun operando con paquetes pequeños. Por lo tanto, el repetidor fullduplex es particularmente adecuado a redes many-to-one. En aplicaciones many-to-many debiera utilizarse un switch, el cual puede proveer un ancho de banda mayor a 1 Gbps.
- Al igual que los dispositivos switch/router Fast Ethernet, los switches Gigabit Ethernet utilizando el estado del arte de la tecnología ASIC, implementarán la capacidad de ruteo a las velocidades máximas del estándar (wirespeed routing) para comunicaciones IP. Los equipos más sofisticados tendrán la capacidad multiprotocolo (IP/IPX). Esta característica es cada vez más importante considerando que el pattern de tráfico 80/20 que representaba la razón de tráfico típica entre tráfico local e intersubred, tiende a igualarse e incluso invertirse.
- Gigabit IEEE 802.3z provee dos estándar para la capa física utilizando fibra óptica (FO) y dos estándar para cable de cobre. Los estándares de FO corresponden a una mejora de la tecnología actual de la especificación ANSI para la capa física de Fibre Channel la cual opera a 1.063 Mbps, tal que pueda operar a 1.250 Mbps y de esta forma proveer el data rate de 1000 Mbps de Gigabit Ethernet. Por ende, Gigabit Ethernet utiliza el mismo esquema de codificación/decodificación para los datos digitales que Fibre Channel, esto es 8B/10B.

Características de los enlaces Gigabit Ethernet.

1000Base-SX

- Pensada para backbones horizontales de hasta 300 m de longitud.
- Utiliza fibra óptica multimodo de 50 um de diámetro y LED de radiación de corta longitud de onda (850 nm).

1000Base-LX

- Para backbones verticales de hasta 550 m de longitud utilizando FO multimodo de 62.5 um de diámetro y LED se larga longitud de onda (1300 nm).
- Para backbones de campus de hasta 5 Km utilizando FO monomodo con diodos láser operando en 1300 nm.

1000Base-CX

- Pensada para los closets de conmutación y salas de computación con un largo máximo de 25 m.
- Utiliza cable twinax, blindado, balanceado, de 150 Ohm.
- Utiliza codificación Fibre-Channel-based 8B-10B.

1000BaseTX

- Utilizará 4 pares de cable UTP categoría 5 con una distancia máxima de 100 m permitiendo redes de hasta 200 m de diámetro.
- NO está aun disponible.

Notas:

- La fibra óptica más utilizada es la graded index MMF 62.5/125 mm (esto es, 62.5 mm fiber optic core y 125 mm outer cladding).
- Para distancias pequeñas se utiliza radiación de 850 nm (shortwave) y el emisor de radiación es normalmente un LED. Para distancias mayores se utiliza radiación de 1300 nm (longwave), normalmente manteniendo el LED como fuente de radiación
- Para fibras monomodo deben utilizarse diodos láser, y el diámetro del núcleo de la fibra puede reducirse de 50 a 9 mm.
- La atenuación típica de FO operando a 850 nm es de 1.5 dB/km y a 1300 nm es de 2 dB/km y de 0.5 a 2 dB por punto de interconexión.
- El ancho de banda y rango de distancias especificado por el estándar, se muestran en la Tabla siguiente:

Estándar	Tipo Fibra	Diámetro (microns)	Longitud de onda (nm)	Ancho de banda (MHz @ 1000 m)	Rango min. (m)
1000 Base-SX	MM	62.5	850	160	2 a 220*
"	MM	62.5	"	200	2 a 275**
"	MM	50	"	400	2 a 500
"	MM	50		500	2 a 550***
1000 Base-LX	MM	62.5	1300	500	2 a 550
"	MM	50	"	400	2 a 550
"	MM	50	"	500	2 a 550
"	SM	9	"	NA	2 a 5000

Notas:

* The TIA 568 building wiring standard specifies 160/500 MHz*km multimode fiber
** The international ISO/IEC 11801 building wiring standard specifies 200/500 MHz*km multimode fiber
*** The ANSI Fibre Channel specification specifies 500/500 MHz*km 50 micron multimode fiber and 500/500 MHz*km fiber has been proposed for addition to ISO/IEC 11801.

4.10.2. Comparación de Tecnologías LAN rápidas.

Los criterios principales de evaluación de las arquitecturas ya descritas serán:

- Disponibilidad y tolerancia a fallas
- Capacidad de transferencia de información
- Escalabilidad que posibilite crecimiento futuro
- Adaptabilidad a cambios tecnológicos
- Estandarización de medios de transmisión y protocolos de transferencia de datos.

4.10.2.1. Fast Ethernet vs. FDDI

En la especificación de backbones de LAN a 100 Mbps, las dos principales tecnologías a considerar son FDDI y Fast Ethernet (FE).

- En un ambiente de backbone conmutado, FE tiene ventajas sobre FDDI ya que provee el doble de velocidad.
- Conexión desde FE o Ethernet a FDDI requiere traducción de los frames con el consecuente mayor retardo y latencia. Esto no sucede al conmutar Ethernet a FE. El performance de una transferencias de datos sostenida, en un ambiente conmutado, está dado por la técnica de arbitración del bus conmutado y la capacidad del backplane del dispositivo. Sin embargo, en conexiones punto-a-punto con FE conmutado CSMA/CD no juega un rol relevante, obteniéndose así su máxima velocidad y estando el performance sólo determinado por la velocidad del dispositivo conmutador (Switch).
- FDDI es capaz de transferir frames más largos por lo que su troughput sería mayor que FE en la transferencia de archivos entre dos servidores en un ambiente compartido. Sin embargo, el tamaño de un frame IP en una red cliente-servidor es, en promedio, entre 200 y 256 bytes. Además, si los clientes son Ethernet, los frames nunca serán más largos que el

- largo máximo Ethernet. Por ello, en este caso los servidores FE tienen el mismo troughput que FDDI y con una latencia menor.
- Pruebas realizadas por la revista Data Communications muestran que manipulando frames de 64 bytes, los adaptadores 100BaseT utilizan el 58% del ancho de banda. Pero en el caso de frames de 1500 bytes utilizan el 99% del ancho de banda, de tal forma que el usuario, servidor o aplicación obtiene el throuhput máximo de 200 Mbps.
- Por lo tanto, los usuarios obtienen un gran aumento de performance al usar 100BaseT fullduplex en servidores de disco, servidores multimedia, conexiones peer-to-peer, y conexiones backbone.
- En un ambiente compartido, FDDI potencialmente ofrece una mejor tolerancia a fallas al utilizar conexiones con anillos duales (FDDI-DAS). Sin embargo, FE también provee alternativas de tolerancia a fallas, a través del Spanning-Tree Protocol (IEEE802.3d), en el cual se mantiene activo sólo uno de dos enlaces redundantes, generándose el swithover en caso de falla. STP tiene la desventaja de ser lento (20 a 30 seg. de retardo). Para failover instantáneo se pueden utilizar transceivers FE tolerante a fallas, los cuales monitorean por hardware el enlace activo y producen el failover de ser necesario. Esta alternativa tiene sólo 1/2 del costo de la interfaz FDDI-DAS.

4.10.2.2. Raw ATM vs IP sobre ATM y FDDI

- En una configuración de nodos back-to-back conectados con un enlace OC-3, Classical IP sobre ATM presenta mayores latencias que aquellas obtenidas usando FDDI, particularmente para mensajes pequeños.
- Sin embargo, para un enlace de la misma velocidad (OC-3), IP sobre ATM vía switches ATM puede exhibir un mejor performance que switches o ruteadores FDDI, debido a la optimización de los switch ATM para celdas de tamaño fijo. Esto indica que ATM es una mejor base que FDDI para implementar comunicaciones internetwork
- Al utilizar Raw ATM, con Fore ATM API y con la capa de adaptación AAL ¾, se obtienen latencias significativamente más bajas que con las configuraciones equivalentes usando IP sobre ATM o FDDI. Esto es lógico, pues en este caso se elimina la capa de emulación y el costo de la emulación asociado.
- Sin embargo el costo de llevar raw ATM hasta el usuario final es mucho más alto que utilizar tecnologías Ethernet, por lo cual actualmente la tendencia es utilizar ATM en el backbone o la interconexión de redes.

4.10.2.3. Gigabit Ethernet vs ATM

- Las conexiones Gigabit Ethernet se espera que serán de menor costo que las interfaces ATM de 622 Mbps (asumiendo idénticas interfaces físicas) debido a la simplicidad relativa de Ethernet y mayores volúmenes de producción. Por ejemplo los dispositivos repetidores Gigabit Ethernet serán significativamente más baratos que conexiones ATM de 622 Mbps, proveyendo alternativas de mayor relación costo beneficio para backbones de redes de datos y conexiones a servidores (ver Tabla 4.3).

Tecnología	Tipo de equipo	1996 Precio/Puerta	1998 Precio/Puerta	Cambio %
Shared Fast Ethernet	Hub	$137	$102	-25%
Switched Fast Ethernet	Switch	$785	$500	-38%
Shared FDDI	Concentrator	$835	$680	-19%
Switched FDDI	Switch	$4000	$3200	-20%
ATM 622 Mbps [1]	Switch	$6600	$4200	-36%
Shared Gigabit Ethernet [2]	Hub	NA	$920 a $1400 [3]	
Switched Gigabit Ethernet [2]	Switch	NA	$1850 a $2800 [3]	

[1] Estimación para fibra multimodo
[2] IEEE goal para fibra multimodo
[3] Estimación Dell'Oro Group e IEEE goals. (2x a 3x Fast Ethernet MM)

- La emergencia de aplicaciones Intranet promueve la migración a nuevos tipos de datos, incluyendo video y voz. En el pasado se pensaba que video requeriría una tecnología de redes diseñada específicamente para multimedia. Esta fue la razón principal que impulsó el desarrollo de ATM, el cual incluye en forma nativa capacidades avanzadas para multimedia, llamadas Quality of Service (QoS). Pero hoy en día es posible mezclar datos y video en redes Ethernet mediante la combinación de los siguientes factores:

  - El aumento de ancho de banda provisto por Fast Ethernet y Gigabit Ethernet, el cual es a su vez aumentado por la técnica de LAN conmutadas y comunicación fullduplex. En efecto, mientras mayor es el ancho de banda, menor es el efecto sobre aplicaciones temporalmente críticas (e.g. transmisión de voz o video) de variables tales como *delay* o *delay variation* (*jitter*).
  - El desarrollo de nuevos protocolos, tal como Resource Reservation Protocol (RSVP), que provee la posibilidad de reservar ancho de banda y por lo tanto de asegurar QoS. Esta posibilidad estaba previamente reservada sólo a Raw ATM.

- El desarrollo de nuevos estándares tales como 802.1Q (priorización) y/o 802.1p (tagging), los cuales proveen facilidades para entregar QoS utilizando información de prioridad explícita para los paquetes en la red.
- Switches sofisticados utilizando las prioridades embebidas en los paquetes por los protocolos antes mencionados, junto con el manejo de colas internas de paquetes, proveerán ruteo con QoS.
- El amplio uso de compresión de video avanzada tal como MPEG-2.

4.10.2.4. Distancias máximas permitidas.

	Ethernet 10 BaseT	Fast Ethernet 100 BaseT	Gigabit Eth. 1000 Base X	FDDI	ATM full duplex
Data Rate	10 Mbps	100 Mbps	1000 Mbps	100 Mbps	155 Mbps
Cat 5 UTP	100 m (min)	100 m	100 m (3)	NA	NA
STP/Coax	500 m	100 m	25 m	NA	100-200 m
Multimode Fiber	2 km	412 m (1) 2 km (2)	200 m (1) 550 m (2)	2 km	
Single-mode Fiber	32 km	20 km	5 km	20 km	800-2000 m

(1) IEEE spec half duplex
(2) IEEE spec full duplex
(3) IEEE 802.3ab bajo studio

4.10.3. Redes de área local virtual (VLANs)

4.10.3.1 Redes LANs compartidas (Shared LANs).

Características:

- La configuración de una LAN está determinada por la infraestructura física que interconecta. Los usuarios se agrupan basados en su ubicación respecto a su Hub de conexión y a como este alambrado el closet principal de interconexiones.
- La segmentación se genera típicamente mediante ruteadores que interconectan los Hubs compartidos.

Consecuencias:

- Este tipo de segmentación no agrupa a los usuarios de acuerdo al grupo de trabajo al que pertenecen o por las necesidades de ancho de banda, ya que por razones de ubicación física, por ejemplo los usuarios del departamento de ingeniería pueden estar conectados al mismo Hub que los usuarios del departamento de administración.

- De esta forma usuarios con diferentes requerimientos de ancho de banda comparten un mismo segmento.
- Además, esta segmentación implica que cada Hub que está conectado a una puerta de un ruteador tiene una dirección de subred diferente. Esto impide una asignación lógica de direcciones de red, generando problemas de seguridad.

4.10.3.2. Redes LAN conmutadas (Switched LANs).

Los problemas asociados a las redes compartidas y la emergencia de switches han originado el reemplazo de la configuración tradicional de LAN por la configuración LAN conmutada.

Características:

- Switches reemplazan los Hubs principales ubicados en el gabinete de comunicaciones.
- Se generan VLAN para proveer la segmentación tradicionalmente provista por ruteadores. La Figura 4.8 muestra la diferencia entre segmentación tradicional y usando VLANs.

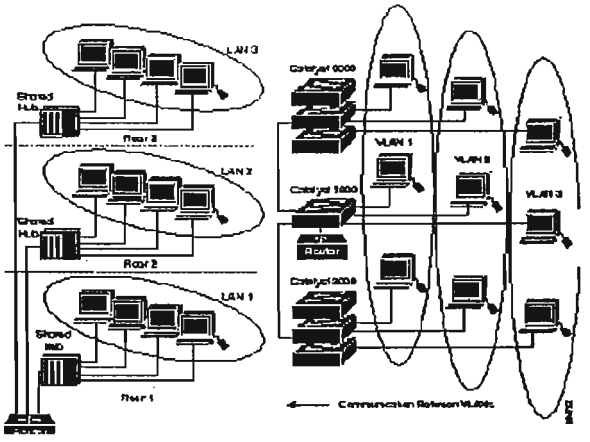


Figura 4.8. Segmentación tradicional de LANs y mediante VLANconmutadas (nm752)

4.10.3.3. Características de una VLAN

- El núcleo de una VLAN es un Switch
- Una VLAN es una red conmutada que está lógicamente segmentada en base a funciones (trabajadores de un mismo departamento), grupos de proyectos o usuarios compartiendo la misma aplicación, sin importar la ubicación física de los usuarios.
- Por ejemplo, cada puerta del switch puede asignarse a una VLAN. Las puertas que no pertenecen a esa VLAN no comparten los broadcast. Esto mejora el comportamiento global de la red.
- La comunicación entre VLANs es provista a través de ruteo de capa 3.
- Agrupando puertas y usuarios a través de múltiples switches, la VLAN puede cubrir un edificio completo, interconectar edificios, o aun redes WAN (ver Figura 4.9)

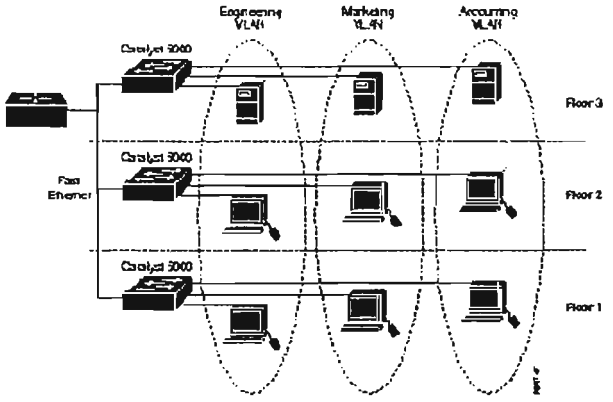


Figura 4.9. Redes definidas logicamente (VLANs) (nm747)

4.10.3.4. Switches, el núcleo de las VLANs

Los switches proveen las siguientes propiedades:

- La inteligencia para realizar filtrado y decisiones de retransmisión de paquetes, basado en métricas de la VLAN definidas por el usuario.
- La habilidad de comunicar información a otros switches o routers en la red.
- En la actualidad, los switches son ubicados entre los segmentos compartidos y los ruteadores ubicados en el backbone. En el futro, desempeñaran un rol importante en la segmentación de VLANs y baja latencia de retransmisión.

4.10.4.5. El rol del Ruteador

- El rol de ruteador cambia desde el rol tradicional de proveer cortafuegos y supresión de broadcast a un control basado en políticas, administración de broadcast y procesamiento/distribución de rutas.
- Los ruteadores siguen siendo vitales para las arquitecturas conmutadas configuradas como VLANs ya que ellos proveen la comunicación entre grupos de trabajo definidos lógicamente.
- Los ruteadores proveen acceso de la VLAN a recursos compartidos tales como servidores o computadores centrales.
- Ellos también proveen la conectividad a otras partes de la red que están lógicamente segmentadas con el esquema más convencional de subredes o permiten el acceso a sitios remotos a través de enlaces WAN.
- La comunicación a nivel de la capa 3, ya sea incorporada en el switch o provista externamente, es una parte integral de cualquier arquitectura conmutada de alto rendimiento.
- Los ruteadores externos se pueden integrar en la arquitectura conmutada con una o múltiples conexiones backbone de alta velocidad (FDDI, Fast Ethernet o ATM). Esta conexiones proveen las siguientes ventajas:

    - Un mayor troughput entre switches y ruteadores
    - Consolidación de un mayor número total de puertas físicas de ruteo para comunicación entre VLANs

4.10.4.6. Beneficios de VLANs

- Reducción de costos de administración relacionados con movimiento, adición o cambios de usuarios.
- Seguridad de la red y grupos de trabajo.
- Actividad de broadcast controlada.
- Reutilización de inversión existente en Hubs.
- Administración y control centralizado.

Reducción de costos de administración
Las compañías continuamente deben reorganizarse para tratar de aumentar la productividad. Por ejemplo, en USA cada año 20 a 40% de la fuerza de trabajo es físicamente reubicada. Estos movimientos, adiciones y cambios son uno de los grandes costos de administración de una red.
Muchos de ellos requieren recableado, Casi todos los movimientos requieren nueva dirección y reconfiguración de Hub o Router. Una VLAN permite compartir la dirección de red sin importar la ubicación física, siempre que su conexión se mantenga a la misma puerta del switch o que la puerta a que esté conectado

(directa o indirectamente) se incorpore a la VLAN en cuestión. Esta situación se muestra en la Fig. 4.10, la cual no requiere ningún cambio de configuración física ni del ruteador.

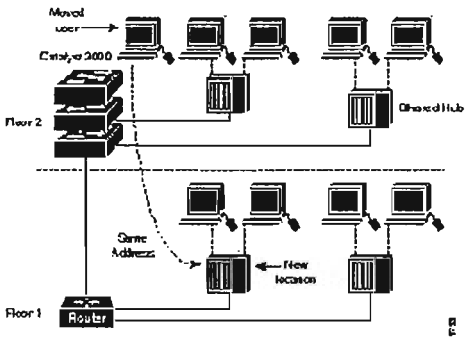


Figura 4.10 Simplificación de los movimientos de usuarios utilizando VLANs (nm753)

4.10.4.7. Control de la actividad de bradcast.

El tráfico broadcast ocurre en toda red y depende de los siguientes factores:

- ❖ Tipo de aplicaciones
- ❖ Tipo de servidores
- ❖ Cantidad de segmentación lógica
- ❖ Uso de los recursos de la red.

- ➢ A pesar de que las aplicaciones se hallan optimizado para minimizar el número de broadcast, las aplicaciones multimedia actuales son intensivas en bradcast o multicast.
- ➢ Los broadcast pueden ser generados también por dispositivos de red o interfaces de red defectuosas.
- ➢ Si no se administran adecuadamente, pueden degradar seriamente el rendimiento de una red completa o incluso dejarlo no funcional.
- ➢ La medida más efectiva contra este problema es segmentar la red adecuadamente incluyendo cortafuegos de protección, provistos usualmente por un ruteador.
- ➢ Por ello se debe considerar que al segmentar un red mediante switches, se pierde el efecto protector de los ruteadores.
- ➢ Pero, al igual que los ruteadores, las VLAN permiten establecer cortafuegos. Estos se pueden crear asignando puertas o usuarios a grupos VLAN específicos ubicados en un mismo switch o múltiples switches interconectados. El VLAN no deja salir el tráfico broadcast fuera de su dominio (ver Fig. 4.11)

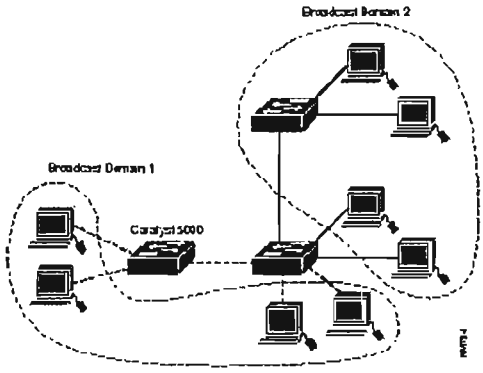


Figura 4.11. Administrando la actividad broadcast mediante VLAs (nm754)

4.10.4.8. Mejor Seguridad de la Red

Una desventaja inherente de una red compartida es que puede ser accedida fácilmente, al conectarse en una puerta cualquiera que esté disponible. Mientras más grande el dominio de broadcast, más vulnerable será la red.
Por ello, una medida simple de aumentar la seguridad es segmentar la red en distintos dominios de broadcast, lo cual permite:

- Reducir el número de usuarios en una VLAN
- Impedir que un usuario de una VLAN diferente se conecte a otra VLAN
- Configurar todas las puertas no utilizadas a una VLAN de bajos privilegios.

Se puede asegurar seguridad adicional usando listas de acceso en el ruteador. (Ver Fig. 4.12)

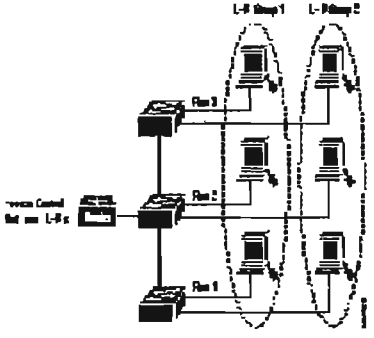


Figura 4.12 Incrementando la seguridad de redes con VLANs (nm755)

4.10.4.9. Definición de Redes Virtuales

Existen cuatro métodos principales de definición de pertenencia a VLAN:

- VLAN por puerto
- VLAN por dirección MAC
- VLAN por filtro
- ELAN o red emulada.

4.10.4.9.1. VLAN por puerto

Cada puerto del conmutador (switch) puede asociarse a una VLAN.

Ventajas:

Facilidad de movimientos y cambios: Un movimiento supone que la estación cambia de ubicación física, pero sigue perteneciendo a la misma VLAN. Requiere reconfiguración del puerto al que se conecta la estación, salvo si se utilizan técnicas de asignación dinámica a VLAN. Un cambio implica pertenencia a una nueva VLAN sin movimiento físico. El puerto del SWITCH ha de configurarse como perteneciente la nueva VLAN y la estación puede precisar reconfiguración de la estación no será necesaria si la subred (IP, IPX, etc.) a la que pertenece está totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar un usuario se traduce normalmente en la reconfiguración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan totalmente está reasignación.

Microsegmentación y reducción del dominio de broadcast: Aunque los switch permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando el rendimiento de las estaciones y se precisan routers o VLANs para aislar los dominios de broadcast. La definición de VLAN por puerto implica que el tráfico broadcast de una VLAN no afecta a las estaciones en el resto de las VLANs, puesto que es siempre interno a la VLAN en la que se origina.

Multiprotocolo: La definición de VLAN por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones. No existen pues limitaciones para protocolos de uso poco común como VINES, OSI, etc. O protocolos dinámicos como DHCP.

Desventajas:

Administración: Los movimientos y cambios implican normalmente una reasignación del puerto del switch a la VLAN a la que pertenece el usuario. Aunque las aplicaciones de gestión facilitan esta tarea es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignan los puertos a la VLAN en función de la dirección MAC o de otros criterios como la dirección de nivel 3.

4.10.4.9.2. VLAN por dirección MAC

La relación de pertenencia a la VLAN se basa en la dirección MAC.

Ventajas:

Facilidad de movimientos: Las estaciones pueden moverse a cualquier ubicación física perteneciendo siempre a la misma VLAN sin que se necesite ninguna reconfiguración del switch.

Multiprotocolo: No presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Desventajas:

Problemas de rendimiento y control de broadcast: Este método de definición de VLAN implica que en cada puerto del switch coexisten miembros de distintas VLANs (se evita el problema si se utilizan puertos dedicados a estaciones pues cada puerto pertenecerá a una única VLAN) por lo que cualquier tráfico broadcast afecta al rendimiento de todas las estaciones. El tráfico multicast y broadcast se propaga por todas las VLANs.

Complejidad en la administración: Todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red en algún tipo de base de datos. Cualquier cambio o nuevo usuario requiere modificación de base de datos. Todo ello puede complicarse extremadamente con redes con un gran número de usuarios o switches.

Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración de forma que las direcciones MAC se copian de las tablas de direcciones de los switches a la base de datos del

servidor. La asignación dinámica de VLAN basándose en direcciones MAC es también posible, aunque su implementación puede ser muy compleja.

4.10.4.9.3. VLAN por filtros

La asignación a las VLANs se basa en información de protocolos de red (por ejemplo dirección IP o dirección IPX y tipo de encapsulamiento). La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de los puertos del switch.

Ventajas:

Segmentación por protocolo: es el método apropiado sólo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en tipo de protocolo de nivel 3 y la segmentación física existente sea muy diferente a los patrones de direccionamiento.

Asignación dinámica: tanto la definición de VLANs por dirección MAC como por protocolo de nivel 3 ayudan a automatizar la configuración del puerto del switch en una VLAN determinada.

Desventajas:

Problemas de rendimiento y control de broadcast: La utilización de las VLANs de nivel 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento global de switch. Los retardos de transmisión pueden aumentar entre un 50% y un 80%.

El problema de control de broadcast surge con las estaciones multiprotocolo o sistema de multistack (por ejemplo estaciones con stacks TCP/IP, IPX y AppleTalk) que pertenecen a tantas VLANs como protocolos utilizan y por lo tanto recibirán todos los broadcast provenientes de las diversas VLANs en las que están incluidas.

No soporta protocolos de nivel 2 ni protocolos dinámicos: La estación necesita una dirección de nivel 3 para que el switch la asigne a una VLAN. Las estaciones que utilicen protocolos de nivel 2 como NETBIOS y LAT no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su router por defecto, el switch no puede clasificar la estación dentro de una VLAN.

Una premisa esencial en la definición de VLANs es que el rendimiento del switch no debe degradarse debido a la existencia de VLANs. Las técnicas de marcado (identificación de paquetes pertenecientes a cada VLAN) utilizadas en la definición de VLANs por puerto permiten mantener una velocidad de transmisión según el ancho de banda disponible (wire speed performance), y por ello ha prevalecido dicha solución en la definición del estándar 802. 1Q.

Estas técnicas permiten además la asignación de un mismo puerto o tarjeta de red a varias VLANs (routers o servidores pueden aprovechar esta ventaja evitándose la utilización de tantas interfaces o tarjetas de red como VLANs existan). ISL (Inter-Switch Link) para Fast Ethernet/Token Ring y 802.10 para FDDI son dos ejemplos de técnicas de marcado.

4.10.4.9.4. ELANs o redes emuladas

La relación de pertenencia a una red emulada es implícita al estándar LANE (LAN Emulation) ya que en el proceso de inicialización del LEC o cliente LANE con sus LECS o servidor de configuración, el servidor le trasmite toda la información necesaria para que el cliente se registre en una determinada LAN emulada (dirección del LES o servidor de LANE, tipo de red emulada, tamaño máximo de paquetes y nombre de ELAN).

Ventajas:

Facilidad de administración: Las funciones de administración se centralizan en el LECS de forma que el administrador puede definir diversos ELANs en la red ATM y asignarlas a puertos de los switches, routers o host ATM independientemente de su ubicación física. Aquellos puertos o host que precisen pertenencer más de una ELAN podrán hacerlo siempre que sus tarjetas ATM soporten más de un LEC.

Facilidad de movimientos y cambios: La pertenencia a una ELAN se mantiene aunque se produzcan movimientos y los cambios de ELAN no suponen ningún cambio físico.

Multiprotocolo: LANE es especialmente un protocolo de nivel 2 sobre ATM y por tanto totalmente independiente de los protocolos de nivel superior.

Desventajas:

Aplicable sólo a Ethernet y Token Ring: LANE define métodos de emulación para Ethernet y Token Ring únicamente. La existencia de tráfico FDDI implica

técnicas de Treanslational Bridging de forma que dicho tráfico es convertido a Ethernet o Token Ring.

No explota la funcionalidad ATM de QoS (Quality of Services) o calidades de servicio y una de las características esenciales de ATM a los protocolos de nivel superior es QoS. Las únicas clases de servicios soportadas por LANE son UBR (Unspecified Bit Rate) y ABR (Available Bit Rate) por ser estas las más cercanas a la naturaleza de los protocolos de nivel MAC. Este inconveniente no es tal comparado con otras técnicas de definición de VLANs dado que el concepto de QoS no se considera en el resto de las definiciones.

Capítulo 5. Diseño y Selección del Equipo que Integrará la Red del Laboratorio de Dispositivos Lógicos Programables.

INTRODUCCION

El presente capítulo tiene como objetivo proporcionar al proveedor, las especificaciones técnicas y los requerimientos funcionales de soporte y servicio, para llevar a cabo la selección del equipo para la red convergente del Laboratorio de Dispositivos Lógicos Programables de la Facultad de Ingeniería de la UNAM. Estas especificaciones técnicas son las mínimas necesarias más no son limitativas.

En esta etapa, se realizará el análisis de las alternativas de implementación y la selección de los recursos necesarios para llevar a cabo este proyecto, por lo que es necesario estudiar distintos aspectos relacionados en cuanto a: Hardware, Software, Humanos e Infraestructura. Además de realizar un análisis de los potenciales riesgos a los que puede estar sometido el sistema una vez implementado; para finalmente, proceder a una selección de éstos de acuerdo al objetivo que la propuesta del proyecto promete.

Serán distintos criterios, funcionales, de costos totales, disponibilidad y principalmente de calidad de servicio, los que harán que la decisión sea a favor de una u otra alternativa.

5.1. Descripción del Laboratorio de Dispositivos Lógicos Programables

Este laboratorio fue creado en 1999. En un principio la mayoría de las computadoras de este laboratorio eran 486 de entre 70 y 250 MB. Ya que el almacenamiento en estas computadoras era muy limitado, existía saturación en ellas ya que los alumnos no borraban sus sesiones. El equipo se fue a bajas de esta universidad y se consiguieron discos duros, memoria RAM, etc.

5.1.1. Finalidad

El objetivo principal de este laboratorio es apoyar en la elaboración de proyectos usando como herramienta principal los dispositivos lógicos programables. Tales como las materias de diseño digital, diseño de sistemas digitales, electrónica digital, organización de computadoras, y arquitectura de computadoras, entre otras.

Otro objetivo es diseñar proyectos los cuales, sirvan como proyecto de tesis a los alumnos de la Facultad de Ingeniería.

El laboratorio además de prestar servicio a los alumnos de la Facultad y a estudiantes de Posgrado, éste desarrolla proyectos tales como:

- Automatización del control de entrada y salida de equipo de cómputo de la Facultad de Ingeniería.
- Tren eléctrico que se detenga en cuatro estaciones utilizando lenguaje AHDL y dispositivos lógicos programables CPLD's.
- Robot móvil seguidor de una línea blanca utilizando lenguaje verilog y dispositivos lógicos programables complejos (CPLD's).
- Grabador de memoria utilizando lenguaje VHDL y dispositivos lógicos programables complejos (CPLD's)
- Diseño e Implementación de un osciloscopio digital didáctico, utilizando dispositivos lógicos programables complejos (CPLDs), con interfaz VGA hacia un monitor de computadora.
- Desarrollo del clon de un micro controlador RISC de la familia PIC de la firma Microchip utilizando lógica programable y lenguaje de descripción de hardware VHDL.

Se han publicado diversos artículos:

- En el SOMI: "Control de un robot móvil mediante una carta ASM programada en verilog."
- En Cracow, Polonia : Development Methodology for digital Measurement instrumentation using programmable logic devices

Además cuentan con Manuales Publicados:

- Entorno de Max-plus II
- Lenguaje de descripción de hardware verilog
- Lenguaje de descripción de hardware VHDL
- Prácticas de laboratorio utilizando dispositivos programables

en este laboratorio se dan cursos curriculares a profesores:

- Programación de Dispositivos Lógicos
- AHDL en aplicaciones de diseños utilizando CPLD's
- Verilog HDL en aplicaciones de diseños utilizando CPLD's
- Aplicaciones de dispositivos lógicos programables
- Programación de Dispositivos Lógicos
- El uso de CPLD's con lenguajes HDL
- Prácticas de dispositivos lógicos programables.
- VHDL en aplicaciones con CLD's.

20.

y cursos a alumnos de la Facultad de Ingeniería:

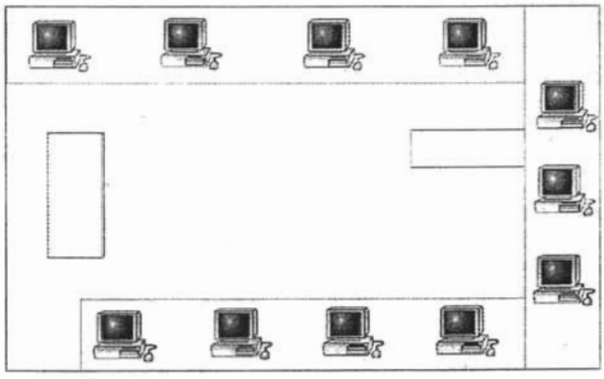
- Introducción a max+plus II.
- Prácticas de dispositivos programables.

- Lenguaje verilogHDL.
- Lenguaje AHDL.
- Lenguaje VHDL.
- Lenguaje de descripción de hardware Verilog y CPLD's
- Lenguaje de descripción de hardware VHDL y CPLD'S

5.1.2. Situación actual de la red

Actualmente el Laboratorio de Dispositivos Lógicos Programables no cuenta con ninguna infraestructura de red, la cual proporcione conectividad entre los equipos que están operando actualmente. Hoy día, el laboratorio cuenta con 11 máquinas. Tiene asignado 2 nodos de red de DGSCA, los cuales darían cabida a la conexión con la red pública Internet.

La misión principal de la red inalámbrica es interconectar todos los equipos para que el usuario no dependa de la computadora que siempre ocupa. Sin importar la terminal, pueda trabajar sus archivos con solo conectarse y transferirlos.



5.2. Análisis y selección de alternativas

A continuación se presentarán los recursos que se necesitarán para llevar a cabo la propuesta de proyecto, sus características, y selección, junto con los criterios o justificaciones respectivas.

5.2.1. Requerimientos

En el último año, las redes han evolucionado drásticamente sobre todo en temas que tienen que ver con tecnología en seguridad en la red,

control de las aplicaciones de la red y ancho de banda sobre todo. Esto, por un lado, ha enriquecido los componentes que integran las redes y por otro se abren nuevas opciones para poder transmitir información a través de ellas. Asimismo un valor importante que ofrece esta evolución de las redes lo representa la reducción de costos y la alta flexibilidad de implementación.

Por dichas razones el Laboratorio de Dispositivos Lógicos Programables busca soluciones tecnológicas que basen su desarrollo en los conceptos anteriores y que por supuesto brinden la mejor relación costo-beneficio y protección de la inversión, así como valores agregados que permitan aprovechar al máximo todas las capacidades de la red inalámbrica y del personal que soporta su administración, todo esto unido a la misión del propio laboratorio.

Los requerimientos son los siguientes:

- El mayor Ancho de banda que proporcione la tecnología inalámbrica para obtener el mayor rendimiento. Esta tecnología deberá estar en el backbone para la comunicación entre todas las computadoras que integran el laboratorio.
- Escalabilidad
- Capacidad de conexión tanto para PCs como para computadoras portátiles.
- Capacidad para enlazarse a Red UNAM.
- Proporcionar comunicación inalámbrica a usuarios móviles a lo largo de todo el laboratorio con conexiones de 11 Mbps y 54 Mbps.
- Mecanismos de seguridad en el AP y a nivel de los usuarios para limitar el uso no autorizado.
- Uso de estándares de redes WLAN.
- Manejo de encripción
- Administración simple, a bajo costo y centralizada.

5.2.2. Conclusiones

En base a lo anterior, se requiere de/que:

- Un equipo que permita una comunicación transparente entre los sistemas de cómputo del laboratorio, en donde su administración se vuelve simple única y de bajo costo.
- Con el sistema requerido se implementará un Sistema de Datos que permita la integración de las nuevas y actuales tecnologías, así como las nuevas aplicaciones requeridas por los usuarios.
- Este sistema solicitado sea un sistema con un rendimiento y operabilidad del sistema de 99.99%.

- Una administración sencilla y centralizada a bajo costo de operación, que pueda realizarse por alguno de los miembros de este laboratorio.
- Acceso en forma inalámbrica para los usuarios móviles por medio del punto de acceso en todo el laboratorio con todo el nivel de seguridad y acceso a la red.
- Proporcione un rango moderado de crecimiento en el número de servicios.
- Ofrezca las más adecuadas y mejores expectativas en esquemas de seguridad a nivel de red.
- El software de administración sea compatible con el sistema operativo Windows 95, 98, ME, XP, 2000 o NT.

5.3. Especificaciones técnicas para los equipos de datos

Se tratan de las especificaciones técnicas del Access Point, que deberá tener las funciones de controlar y garantizar el flujo local de toda la información de los usuarios, de tarjetas inalámbricas para las PCs y, en caso de requerirse, de tarjetas PCMCIA para las computadoras portátiles.

5.3.1. Acceso inalámbrico

Estos equipos deberán tener las siguientes funciones:

- Proporcionar acceso mediante un "Access Point" a los equipos de cómputo con comunicación inalámbrica mediante el estándar IEEE 802.11.
- Controlar remotamente el acceso a través de la red y permitir remotamente su monitoreo y administración para garantizar la seguridad de la red y mantener la operación continua de la red inalámbrica.
- Deberán tener la opción a conectarse a la infraestructura de la red de datos de la UNAM.

5.3.2. Características mínimas que debe cumplir el equipo.

- Punto de acceso responsable de transmitir y recibir información bajo tecnología de radio frecuencia y entregar información bajo las tecnologías de transmisión Ethernet y TCP/IP.
- El equipo de tecnología inalámbrica deberá de ser conectado utilizando el cableado y la infraestructura de la red de datos.
- El equipo deberá contar con la capacidad de poder transmitir información de datos tanto a 11Mbps como a 54 Mbps.

- El software del sistema y el firmware del equipo deberán poder ser migrados a nuevas versiones de manera remota y local en las instalaciones del cliente.
- El equipo deberá tener la capacidad de ser reiniciado (reset) a través de comandos de software.
- La configuración entera del dispositivo (conexiones, configuración de puertos, etc.) deberán poder ser almacenadas en su totalidad en un archivo en la estación de administración y monitoreo. Este mismo archivo deberá poder ser descargado en el mismo nodo o en un nodo de reemplazo a través de comandos de software.
- La configuración del nodo deberá conservarse en el equipo aún cuando se haya apagado el equipo por falla de energía.
- El equipo deberá incluir la(s) antenas y cableado necesario para su total operación.
- El equipo deberá de poder hacerse visible a los clientes inmediatamente al suministrarle potencia eléctrica y sin necesidad de configuración adicional.
- El equipo deberá contar con la opción para ser restablecido de manera automática en caso de una falla de energía eléctrica y sin la necesidad de una intervención manual del personal de laboratorio.
- El equipo deberá contar con la característica de poder censar los canales RF activos en la red y automáticamente configurarse en un canal que no interfiera la transmisión de los otros puntos de acceso en producción.
- El equipo deberá contar con 2 antenas intercambiables para lograr una mejor cobertura.
- Para el caso del radio 802.11b, el equipo deberá contar con la capacidad de poder conectarle antenas direccionales, omnidireccionales u omnidireccionales de 2, 4 u 8dbi y que sean compatibles con el hardware del equipo para mejorar la recepción y transmisión (cobertura) de acuerdo a las necesidades.
- El equipo deberá de conectarse a la red con un puerto 10/100 Mbps.
- El equipo deberá de contar con 2 slot mínimo tipo mini-pci a manera de poder combinar cualquier tipo de radio inalámbrico 802.11b, 802.11a y 802.11g y poder ser actualizable a cualquier tecnología futura solo agregando el componente de software correspondiente.
- El equipo deberá de soportar el modo Turbo 802.11a (108 Mbps) para conexiones con radio 802.11a.
- El equipo deberá de contar con LED's que provean las condiciones siguientes:
  - ✓ Poder: Si el equipo está conectado a la alimentación.
  - ✓ Inalámbrico: Cuando hay conexión con otro equipo y hay comunicación.
  - ✓ Ethernet: Cuando hay conexión a la red de datos y si hay actividad.

- El equipo deberá de tener la capacidad de soportar al menos 20 usuarios conectados simultáneamente en el Punto de Acceso utilizando aplicaciones como correo electrónico, http, etc.
- El equipo deberá de poder ser administrado a través de interfaz web con una conexión segura a través de SSL y adicionalmente bajo el software de administración propio del equipo que deberá estar basada en una aplicación gráfica.
- El software de administración del equipo deberá poder ser instalado en computadoras que corran Windows 95, 95B, 98, ME,2000 o NT 4.0 o XP.
- Todos los equipos deberán poder ser administrados desde una sola estación de Administración o Monitoreo ya sean locales o remotos.
- El software permitirá realizar gráfico y remoto lo siguiente:
  - ✓ Leer y salvar configuraciones.
  - ✓ Restaurar configuraciones.
  - ✓ Realizar actualizaciones del firmware del Access Point.
  - ✓ El equipo deberá de contar con algún software que permita ayudar a determinar la mejor localización para cada punto de acceso y permita asimismo calcular el número de puntos de acceso necesarios para obtener suficiente ancho de banda y cobertura.
  - ✓ El equipo deberá de contar con niveles de seguridad para proteger la información de la red de observadores no autorizados sin necesidad de cambiar o agregar componentes y sin costo adicional.
  - ✓ El equipo deberá de dar de baja de su lista actual de clientes a los clientes que ya no se encuentren asociados al access point o que no están transmitiendo más a través de éste.
  - ✓ El equipo deberá de poder filtrar usuarios por dirección MAC o por nombre y contraseña.
  - ✓ El equipo deberá de tener la capacidad de deshabilitar el broadcast del ESSID.
  - ✓ El equipo podrá brindar la posibilidad de bloquear la comunicación entre clientes asociados al mismo access point, así como bloquear la comunicación para administrar el equipo a cualquier usuario que no tenga este perfil.
  - ✓ Deberá manejar al menos encripción de 40/64/128/154 bits tipo WEP.
  - ✓ El equipo deberá de tener la capacidad de encripción tipo WPA.
  - ✓ El equipo deberá de soportar autenticación de usuarios a través del estándar 802.1x y RADIUS.
  - ✓ El equipo deberá de contar con claves de encripción dinámicas de 128 bits por cada sesión que se negocian automáticamente entre los clientes y el punto de acceso, además de poder utilizar llaves de encripción estáticas de 128

bits.

- Estándares soportados:
  - ✓ IEEE 802.11b, 802.11a y 802.11g
  - ✓ IEEE 802.1x
  - ✓ Certificación Wi-Fi
  - ✓ Bridge 802.3
  - ✓ 10/100 BASE-T
  - ✓ Clear Channel Select
  - ✓ Dynamic Rate Shifting
  - ✓ Encripción 40,128 y 154 bit WEP, con llave compartida
  - ✓ Encripción WPA
  - ✓ TCP/IP, Netbeui, IPX
  - ✓ Autenticación por EAP-MD5 y EAP-TLS, EAP-TTLS, PEAP, TKIP
  - ✓ HTTPS
  - ✓ TFTP
  - ✓ SNMPv1, SNMPv3
  - ✓ Soporte de Radius
  - ✓ Soporte de SNTP

5.3.3. Requerimientos mínimos para tarjetas inalámbricas para equipos portátiles

- Bus PCMCIA.
- Antena retráctil que activa el modo de "power mode" o conectividad inalámbrica.
- Controladores para Windows 2000, Me, Windows 98SE, Windows 98, XP.
- Capacidad de conectarse al access point que ofrece mejor calidad de señal dentro de una red inalámbrica.
- Conexión inalámbrica con cobertura hasta de 20 metros.
- IEEE 802.11b, 802.11a y 802.11g.
- Velocidad de 11, 54 y 108 Mbps con censado automático de velocidad.
- Soporte de Modo Turbo.
- Certificado Wi-Fi de interoperabilidad.
- Soporte de Protocolos TCP/IP, NetBEUI, DHCP.
- Soporte de encripción 40, 128 y 154 bits WEP, con llave compartida sin necesidad de cambiar o agregar componentes y sin costo adicional.
- Soporte de 802.1x.
- Soporte de EAP-MD5 y EAP-TLS, EAP-TTLS, PEAP, TKIP.
- Soporte de software de administración para conexión en modo ad-hoc.

- Las tarjetas deberán de soportar las nuevas funcionalidades de inalámbrico sólo con la actualización del firmware de la misma tarjeta.
- CD que incluya controladores de instalación, software o equipo de diagnóstico y documentación.
- Guía de referencia o manual de usuario.
- 2 años de garantía.
- Las tarjetas deberán ser del mismo fabricante de los Access Points.

5.4.1 Selección de equipo

La siguiente tabla muestra los parámetros más importantes del equipo de cada fabricante para ser seleccionado como los dispositivos que centralicen el flujo de información de la red y que ofrezcan los servicios de red a cada usuario.

5.4.1. Access Point

Características	SMC2870W	AP8750 de 3com	TEW-450APB
Banda de Frecuencia	2.4GHz	• 802.11a: 5 GHz • 802.11g: 2.4 GHz	2.4 ~ 2.484 GHz
Tipo de Modulación	• BPSK, QPSK, DBPSK, DQPSK, CCK, • 16QAM, 64QAM	• 802.11a: OFDM • 802.11b: CCK, DQPSK, DBPSK • 802.11g: OFDM y DSSS (con codificación Barker y CCK para compatibilidad con 802.11b)	• 802.11b: CCK, DQPSK, DBPSK • 802.11g: OFDM
Velocidad	• 802.11b: 1/2/5.5/11 Mbps • 802.11g: 6/9/12/18/24/36/48/54 Mbps	• 802.11a: hasta 54 Mbps • 802.11b: 1/2/5.5/11 Mbps • 802.11g: 6/9/12/18/24/36/48/54 Mbps	• 802.11b: 11/5.5/2/1Mbps • 802.11g: 54/48/36/24/18/12/9/6Mbps • SuperG: 108Mbps
Seguridad	• 64-bit/128-bit Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • 802.1x authentication • Disable SSID Broadcast • MAC Address Filtering	• 64-bit/128-bit/152 bit Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • 802.1x authentication con RADIUS • Advanced Encryption Standard (AES) • Disable SSID Broadcast • Extensible Authentication Protocol (EAP) • MAC Address Filtering	• 64/128-bit WEP protect Access Point from unwanted wireless clients. • WPA(Wi-Fi Protected Access)/WPA-PSK • Advanced Encryption Standard (AES) • TKIP • ESSID Control • Filtrado de MACs
Rango y/o Desempeño	• 802.3, 802.3u • 802.11b • 802.11g	• 802.3af • 802.11a • 802.11b/g	• Wired: ▪ IEEE 802.3 (10Base-T) ▪ IEEE 802.3/802.3u (100Base-TX) ▪ ANSI/IEEE 802.3 Auto Negociación • Wireless: ▪ IEEE 802.11b (11Mbps) ▪ IEEE 802.11g (54Mbps)

Estándares	• Direct Sequence Spread Spectrum (DSSS) • Orthogonal Frequency Division Multiplexing (OFDM)	• Direct Sequence Spread Spectrum (DSSS) • Orthogonal Frequency Division Multiplexing (OFDM)	• Direct Sequence Spread Spectrum (DSSS) • Orthogonal Frequency Division Multiplexing (OFDM)
Tecnología de Radio	• 802.11b: 1/2/5.5/11 Mbps • 802.11g. 6/9/12/18/24/36/48/54 Mbps	• 802.11a: 54/48/36/24/18/12/9/6Mbps (hasta 108 Mbps en modo turbo) • 802.11b: 1/2/5.5/11 Mbps • 802.11g: 6/9/12/18/24/36/48/54 Mbps	• 802.11b: 11/5.5/2/1Mbps • 802.11g: 54/48/36/24/18/12/9/6Mbps • SuperG: 108Mbps
Tasa de datos	• 10/100 Mbps RJ-45 port	• 10/100 Mbps RJ-45 port	• LAN : 1 x 10/100Mbps Auto-MDIX Port
Interface	• 2 antenas externas dipole	• 2 antenas externas dipole	1(x 2dBi) antena externa dipole con conector hembraSMA
Antenas	• Power • Transmit / Receive (Wireless) • Transmit / Receive (Wired)	• Radio • Power • Ethernet • Radio (2o radio instalado)	• Power • LAN • WLAN
LEDs	AC Input: 100-240V 1A DC Output: 5V 2A	PoE: Energizado por el Puerto Ethernet	5V DC, 2A Adaptador externo
Voltaje de Operación	• -20Co to 40Co (-4Co to 104Co)	• -15° C to 40° C (59° F to 104° F)	• 0°~ 55° C (32°F~ °F)

Temperatura de Operación	• -20Co to 40Co (-4Co to 104Co)	• 5-95% non-condensing	• Max. 95% (non-condensing)
Humedad de Operación	• 161mm x 30mm x 119mm	Height: 320 mm Width: 200 m Depth: 70 mm	• 146 x 113 x 41 mm (sin antena)
Dimensiones	• 195g (6.87oz)	287g (4.86 oz)	• 118g. (0.26 lb)
Peso			

La evaluación y selección del dispositivo de interconexión se hará por medio de los atributos que están basados en las necesidades y requerimientos de la red del Laboratorio de Dispositivos Lógicos Programables.

Por lo tanto:

- El Access Point de 3com queda totalmente descartado ya que requiere ser energizado por el puerto RJ-45 y todavía no está contemplado conectar la red del laboratorio a RedUNAM. Con lo cual implicaría que DGSCA entregara energizado dicho nodo. Es decir, se necesita alimentación de corriente aparte.
- En cuanto al desempeño de los equipos de Trend Net y 3com, su capacidad está muy sobrada para los 11 equipos que se piden interconectar. El área de radiación es muy extensa comparado con lo que mide el laboratorio.

Por consiguiente, éstos equipos no serán aprovechados al máximo. El Access Point de SMC es la solución más adecuada para centralizar el flujo de información y dar los servicios de red a los usuarios, por lo siguiente:

- Proporciona un rango moderado de crecimiento en el número de servicios.
- Tiene alimentación de energía independiente.
- El área de radiación es relativamente más pequeña en comparación con los otros 2 equipos, pero que se ajusta al área del laboratorio.
- Simplifica y reduce costos de la administración, operación y mantenimiento.
- Ofrece las más adecuadas y mejores expectativas en esquemas de seguridad a nivel de red.
- El software de administración es compatible con computadoras que corran Windows 95, 98, ME, XP, 2000 o NT.

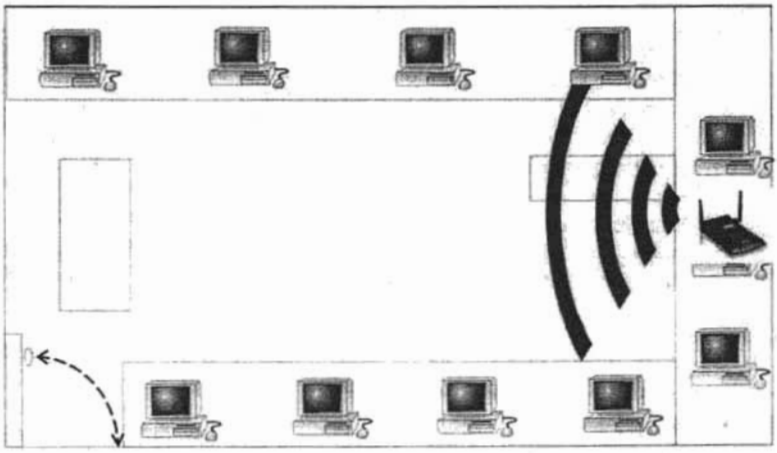
5.4.2. Tarjetas inalámbricas para las computadoras personales y portátiles

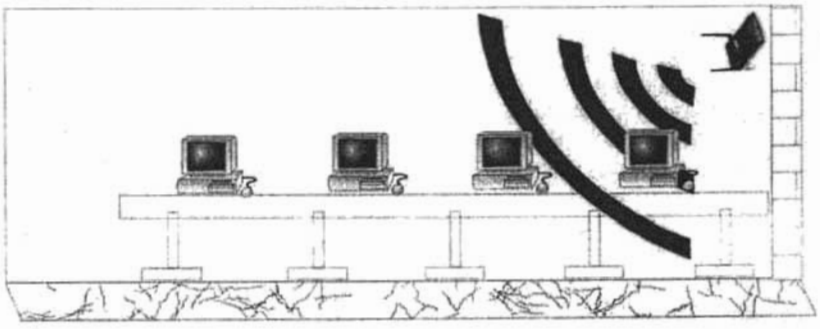
Características	Tarjetas PCI para PCs	Tarjetas PCMCIA para LAP TOPs
Interface	32-bit PCI 2.2 Bus Master	• 32-bit Cardbus con PCMCIA Type II
Estándares	• IEEE 802.11a (opcional) • IEEE 802.11b • IEEE 802.11g	• IEEE 802.11a (opcional) • IEEE 802.11b • IEEE 802.11g
Antenna	1 x 2dBi Detachable Dipole Antenna	Preferentemente, antena retractable
Sistemas Operativos Soportados	Windows 98(SE), ME, 2000, XP(SP1/SP2), 2003 Server	Windows 98(SE), ME, 2000, XP(SP1/SP2), 2003 Server
Técnica de modulación	• 802.11b: CCK (11 and 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) • 802.11g: OFDM	• 802.11b: CCK (11 and 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps) • 802.11g: OFDM
Banda de Frecuencia	• 802.11a: 5 GHz (opcional) • 802.11g: 2.4 GHz	• 802.11a: 5 GHz (opcional) • 802.11g: 2.4 GHz
Tasa de datos	• 802.11a: 54/48/36/24/18/12/9/6Mbps (hasta 108 Mbps en modo turbo) (opcional) • 802.11b: 1/2/5.5/11 Mbps • 802.11g: 6/9/12/18/24/36/48/54 Mbps	• 802.11a: 54/48/36/24/18/12/9/6Mbps (hasta 108 Mbps en modo turbo) (opcional) • 802.11b: 1/2/5.5/11 Mbps • 802.11g: 6/9/12/18/24/36/48/54 Mbps
Seguridad	• 64-bit/128-bit/152 bit Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • 802.1x authentication con RADIUS • Advanced Encryption Standard (AES) • Disable SSID Broadcast • Extensible Authentication Protocol (EAP) • MAC Address Filtering	• 64-bit/128-bit/152 bit Wired Equivalent Privacy (WEP) • Wi-Fi Protected Access (WPA) • 802.1x authentication con RADIUS • Advanced Encryption Standard (AES) • Disable SSID Broadcast • Extensible Authentication Protocol (EAP) • MAC Address Filtering
Canales	1~14 Channels (Universal Domain Support)	1~14 Channels (Universal Domain Support)

Nota: La propuesta de las características de las tarjetas de red para los equipos de cómputo se debe considerar como una idea para su selección y dependerá totalmente de la decisión del encargado del equipo, considerando otros modelos de equipo de red de fabricantes no contemplados en este trabajo.

5.5. Diseño e implementación

Como en el diseño debemos mostrar la conexión que se pretende realizar, además de los productos que se utilizaran, los cuales ya fueron vistos anteriormente. Se muestra a continuación como sería la red inalámbrica.





5.6. Administración y monitoreo de la red

El sistema deberá ser administrado desde cualquier estación de la red (local o remotamente) que se seleccione para Administración y Monitoreo, mediante el protocolo HTML/Web. El equipo debe contar en su arquitectura con componentes adecuados que no afecten su desempeño, es decir, componentes que no sean un cuello de botella en el funcionamiento y que pueda llegar a simular un bajo desempeño de la red a los usuarios finales. Estos componentes son: la velocidad del procesador, el subsistema de disco duro, la memoria RAM y la tarjeta de interfaz de red (NIC).

5.6.1. Equipo servidor

Para las funciones de administración y monitoreo de los equipos activos, en la arquitectura el equipo que se desempeñe como servidor se debe considerar las características de los siguientes componentes:

Procesador
La velocidad del procesador es un factor importante en el desempeño del servidor. El procesador debe satisfacer la carga de trabajo que demanda la tarjeta de interfaz de red para el procesamiento de los paquetes de datos que se reciben y se envían, además de las peticiones de procesamiento que demanda el sistema operativo de red y la plataforma de administración y monitoreo.

Subsistema de Disco Duro
El subsistema de Disco duro consiste en el disco duro en sí y el controlador de disco que manipula la transferencia de datos entre el disco y el procesador del equipo. Si el subsistema de disco no provee acceso rápido a los archivos almacenados en este, los usuarios finales esperarán demasiado tiempo para los requerimientos de procesamiento de estos archivos. El rango de transferencia de datos, o la velocidad con que se pueden transmitir datos entre el subsistema de disco y el procesador, es una función del disco mismo, del controlador del disco y de las interfaces de bus entre el disco y el controlador del disco y entre el controlador del disco y el procesador. La rapidez de estos componentes son: la rapidez de tiempo de respuesta de la red en los equipos terminales. El subsistema de disco debe experimentar un alto desempeño para los requerimientos del servidor de lectura y/o escritura de datos, y el tiempo de espera de entrada y salida de datos en el disco (disk input/output) debe ser mínima.

Memoria RAM
La memoria caché de red del servidor son los datos mas recientes de acceso en la memoria. Cuando en el servidor se llena la capacidad de memoria RAM, esta escribe los datos de último acceso a disco duro

(swapping). Si el servidor tiene una configuración de memoria RAM escasa experimentará largo tiempo de espera para acceder a los datos en disco, ya que la lectura de datos desde controladores de disco es sustancialmente más lenta que la lectura de datos desde la memoria RAM. La velocidad de lectura a la memoria RAM también afecta en general al desempeño del servidor.

Tarjeta de interfaz de red (NIC)
Las tarjetas de interfaz de red pueden también afectar el desempeño de red en el servidor. Las tarjetas de red varían en costo y desempeño, sin embargo, es importante evaluar las siguientes características:

- Data Throughput. Esta es la velocidad en la cual la tarjeta de interfaz de red transfiere datos entre la memoria del equipo y la red. El data throughput depende del ancho de la interfaz de bus al procesador del servidor y del método que la tarjeta de red usa para transferir los datos. La capacidad de envío de datos en los buses comúnmente es de 8, 16 y 32 bits. La rapidez con que una tarjeta de red puede transferir datos depende del tamaño del bus de datos al procesador. Actualmente existen arquitecturas de tarjetas de red que ofrecen diferentes extensiones de bus, pero para este caso una opción sería las tarjetas con arquitectura PCMCIA (Personal Computer Memory Card International Association) las cuales operan con un buses de 32 bits.

    - ✓ Las tarjetas de interfaz de red transfieren datos a la memoria del servidor usando uno de los tres métodos: direct memory mapping, input/output ports ó direct memory addressing (DMA). El método direct memory mapping es usualmente el método de transferencia de datos más rápido.

- Onboard processor. Las tarjetas de interfaz de red utilizan un eficiente microprocesador en la tarjeta que puede mejorar su desempeño, y por lo tanto de la red.

- Soporte de Controladores (Drivers). Los controladores son líneas de código que traducen las llamadas de los programas redirectores de red en instrucciones para la tarjeta de red. Los problemas con controladores mal programados y con escaso soporte, afectan directamente al desempeño del enlace de red de los equipos que va desde las retransmisiones necesarias para enviar un paquete, tiempos de espera extensos para envío y recepción de datos, y pérdida de conexiones.

Considerando las características anteriores, en la arquitectura del servidor de administración y monitoreo, se puede establecer que el servidor no sea un cuello de botella en el tiempo de respuesta de la red que puedan experimentar los usuarios o administradores.

Para la administración de las aplicaciones de escritorio se requiere de computadoras que cumplan las características de arquitectura antes descritas y funcionen como servidores que centralicen en cada área de trabajo de la Torre ciertas aplicaciones y servicios de escritorio y la administración de recursos de hardware y software, además de un equipo servidor de administración y monitoreo de todos los servidores de aplicaciones y equipos de escritorio. Los servidores de aplicación deben ofrecer los servicios de seguridad en las aplicaciones de escritorio como lo son: autenticación de usuarios, confidencialidad, integridad de los datos y la administración de llaves para la autenticación de los usuarios y evitar accesos no autorizados.

5.6.2. Sistema de administración, mantenimiento y operación

El control y monitoreo centralizado de los dispositivos activos permite obtener un diagnóstico de fallas y control de recursos que pueden simplificar la administración y mantenimiento de la red, pero básicamente a mantener esquemas de seguridad y confiabilidad a nivel de red. La plataforma de administración sirve para que el administrador de la red pueda consultar la información en diversos formatos y utilizar métodos estadísticos para evaluación de cómo están siendo utilizados y aprovechados los recursos de la red, el rendimiento que esté ofreciendo, detectar las posibles fallas y encontrar pronta solución a éstas teniendo como base de conocimiento lo que las ocasiona.

La tarea específica de monitoreo permite la extracción e interpretación de datos relacionado con el estado de los dispositivos conectados a la red. El desarrollo de una buena función de monitoreo permite llevar a cabo una planeación de posibles crecimientos de la red, esto de la manera más adecuada basada en diseños y datos estadísticos. En conclusión, se puede establecer que para facilitar las tareas de administración es importante la incorporación de una plataforma de administración, mantenimiento y monitoreo.

Conclusiones

Lo anterior ha delineado lo que es una red inalámbrica y lo que implica la instalación de la misma. La tecnología WLAN es una tecnología madura, perfectamente aplicable y funcional hoy en día a un costo accesible pero haciendo especial hincapié, en que si se decide implantar, se deben tomar medidas de seguridad. En esta tesis se plantea el diseño de una red inalámbrica tomando en cuenta las necesidades del Laboratorio de Dispositivos Lógicos Programables. El laboratorio es pequeño y el número de PC's por el momento también es pequeño por ende se decidió la implementación del Access Point SMC ya que este es el que se ajustaba y satisfacía las necesidades. Entre las medidas de seguridad que se tomaron, las más básicas son una correcta configuración de la red para impedir el acceso a la misma de usuarios no autorizados y hacer que la información circule de forma cifrada.

Asegurar una red no es un proceso fácil, y no existe una receta simple para hacerlo. Sin embargo desde mi punto de vista, los siguientes puntos básicos siempre nos ayudarán para lograr este propósito:

1) **Seguridad física**: El primer paso para considerar una red segura, es asegurarla físicamente (tanto para evitar intrusiones como para asegurar la conectividad). Me explico, es necesario:

    a. Permitir que la red crezca con un plan.
    b. Crear una infraestructura apta para llevar el cableado.
    c. Atenerse completamente a los estándares propuestos por los fabricantes.
    d. Mantener la claridad y limpieza en todos los puntos importantes de nuestro proyecto.

No podemos dejar de lado, claro está, el mantener un registro actualizado de dónde tenemos instalados puntos de red, a quién pertenece, la dirección MAC (dirección física del adaptador de red) de los dispositivos que ahí conectemos, y siempre que sea posible no instalar puntos en espacios públicos, ya que para un intruso es muchas veces mucho más fácil conectarse a través de la red local que buscar el acceso remotamente.

Si tenemos una red inalámbrica es mucho más difícil asegurar físicamente nuestra red. De todos modos, utilizando las capacidades de cifrado de las redes inalámbricas, como las que se mencionaron aquí, ubicando nuestros puntos de acceso tan al centro de nuestras instalaciones como sea posible para evitar "derramar" señal, y en general utilizando el sentido común al instalar nuestra red, podremos evitar exponernos de más.

Una red inalámbrica puede ser muy conveniente y económica, pero si es instalada sin el cuidado necesario, puede ser nuestra mayor vulnerabilidad.

2) **Seguridad perimetral**: Una vez que tenemos confianza en nuestra instalación de red, tenemos que definir perímetros de seguridad, los cuales serán divididos por uno o varios firewalls. La configuración más simple consiste en solamente poner un firewall entre nuestra red local y nuestra salida a Internet, permitiendo únicamente la entrada y salida a las conexiones autorizadas. Por las características del laboratorio no fue necesario definir una seguridad perimetral debido que la red inalámbrica solo se utilizara para la conexión de los equipos para transferir información entre ellas, es decir; no salen a Internet.

3) **Monitorear constantemente la red**: Parte importante de la seguridad en la red consiste en monitorearla activamente. Hay muchas condiciones que pueden llevarnos a fallas, y muy fáciles de corregir -o por lo menos diagnosticar- si contamos con herramientas de monitoreo. Podemos utilizar herramientas libres como MRTG, que nos da un reporte gráfico -diario, semanal, mensual y anual- de los datos que le configuremos.

Otro aspecto importante a monitorear son los intentos de ataque que estemos recibiendo, para saber de qué protegernos, cuáles son nuestros principales riesgos, quién está intentando atacarnos, por qué medios, y qué es lo que buscan. Para ello, podemos instalar sistemas de detección de intrusos (IDSs, por sus siglas en inglés). El IDS más poderoso y popular hoy en día es libre, y se llama Snort.

4) **Mantener las computadoras al día**: La instalación de nuestra red puede haber sido muy segura. Podemos tener firewalls delimitando cada área específica. Sin embargo, si no mantenemos actualizados nuestros sistemas operativos, programas y herramientas, nuestra red no podrá ser considerada segura. Es muy frecuente, en software tanto libre como propietario, que sean encontradas fallas de programación que pueden traducirse en agujeros de seguridad - un administrador de redes responsable debe mantener los sistemas con los parches al día, para no sufrir ataques prevenibles.

Las redes inalámbricas pueden tener y están teniendo mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria, como ya se dijo es relativamente fácil el crear una red híbrida, porque seguiríamos teniendo las ventajas de la velocidad que nos brinda la parte cableada y expandiríamos las posibilidades con la parte inalámbrica.

Concluiría haciendo hincapié en las carencias que se tienen en nuestra Universidad, un ejemplo claro es este laboratorio. Esta tesis a planteado la necesidad de realizar una actualización, desafortunadamente por problemas de dinero no se ha logrado este propósito.

La tecnología esta avanzando a pasos agigantados mientras nuestras instalación se están quedando obsoletas, nada mas basta con compararnos con cualquier universidad que esta consiente de las necesidades de los alumnos y veremos que nosotros seguimos en la prehistoria, es indispensable una actualización para poder crear una universidad de primer mundo

Bibliografía.

LIBROS

Uyless Black; Computer Networks Protocols, Standard and Interfaces; Prentice Hall 1992

Michael Santifaller; TCP/IP and NFS (internetworking in Unix Enviroment); Addison Wesley 1991

Alfred Halshall; Data Communications, Computer Networks and Open Systems 3a. edición; Addison Wesley 1994

José Carbajal; WI-FI Cómo construir una red inalámbrica; 2004 AlfaOmega Grupo Editorial, S.A de C.V

Tanenbaum, Andrew S.; Computer networks, Upper Saddle River, New Jersey : Pearson Education, c2003 4th ed.

TESIS

Hernández Campos, Gabriela; Redes inalámbricas; Universidad Nacional Autónoma de México. Escuela Nacional de Estudios Profesionales Aragón

Vargas Jiménez, Alex Jonathan; Tendencias de las redes inalámbricas en México wpan, wlan, wman; Universidad Nacional Autónoma de México, UNAM

Calzada Ríos, Carlos Gilberto; Redes inalámbricas; Universidad Nacional Autónoma de México. Facultad de Ingeniería

DIRECCIONES WEB

Fabricantes:

3Com Corporation; www.3com.com

Cabletron Systems Inc.; www.cabletron.com

Bay Networks Inc.; www.baynetworks.com

Cisco Systems Inc.; www.cisco.com

SMC Networks; http://www.smc.com

Organizaciones y Forums:

Institute Ethernet Alliance; www.ieee.org

Wireless LAN Association; The Wireless Networking Industries Information Source http://www.wlana.org

WIFI Aliance; http://www.wirelessethernet.org/

http://www.hiperlan2.com/
Bluetooth, The Official Bluetooth Website; http://www.bluetooth.com/

Revistas:

Network Computing; www.networkcomputing.com

LAN Times Magazine; www.lantime.com

Network World; www.nwfusion.com