UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POST-GRADO

OPTIMIZACION DE DISPOSITIVOS UTILIZANDO RUTEADORES EN UNA RED PARA SU APLICACION EN SISTEMAS ALAMBRICOS E INALAMBRICOS

POR

JUAN CARLOS DONJUAN LOPEZ

TESIS

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERIA CON ESPECIALIDAD EN TELECOMUNICACIONES

ENERO 2008

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POST-GRADO

OPTIMIZACION DE DISPOSITIVOS UTILIZANDO RUTEADORES EN UNA RED PARA SU APLICACION EN SISTEMAS ALAMBRICOS E INALAMBRICOS

POR

JUAN CARLOS DONJUAN LOPEZ

TESIS

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERIA CON ESPECIALIDAD EN TELECOMUNICACIONES

ENERO 2008

INDICE

CAPITULO 1

INTRODUCCION

1.1 Planteamiento del Problema

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 las computadoras, así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos, 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 las computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo equipo de cómputo para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con mayor rapidez por otro que considera un número grande de computadoras separadas, pero interconectadas, que efectúan el mismo trabajo. Estos sistemas se conocen con el nombre de redes de computadoras.

Las redes en general consisten en compartir recursos, y uno de sus objetivos principales es hacer que todos los programas, información y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso o del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000km de distancia de la información, no debe evitar que este la 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.

Un tercer objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Dentro de las ventajas que encontramos entre ambos equipo a grandes rasgos tenemos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este último objetivo siempre ha sido punto importante al momento de implementar o actualizar redes de cómputo ya existentes.

En nuestro proyecto de investigación se optimizarán algunos de los dispositivos de comunicación instalados en una red de computadoras ya existente de tal forma que permita la compatibilidad con la nueva tecnología inalámbrica incluida en la mayoría de los nuevos equipos de cómputo móviles y de escritorio existentes hoy en día, así como la de utilizar de manera eficiente la infraestructura de cableado estructurado ya instalado en nuestras instalaciones de trabajo.

La principal problemática identificada en nuestra red de datos actualmente instalada, que utilizaremos para nuestro estudio, radica en gran medida en el equipo de comunicaciones utilizado para compartir el enlace dedicado a Internet. El equipo en cuestión ha venido generando una serie de problemas con la conexión al servicio de Internet y nuestra red de computadoras existente. Se busca que la mejora al sistema ayude a resolver los conflictos ocasionados por dicho equipo, cuyo desempeño ha ido disminuyendo rápidamente con el paso de los años.

1.2 Objetivo

1.2.1 Objetivo General

Optimizar algunos dispositivos con los que cuenta actualmente una red de computadoras para mejorar la eficiencia de la misma.

1.2.2 Objetivos Específicos

- Comprobar que la función de un equipo proxy puede ser sustituida por un equipo de ruteo en redes locales pequeñas.
- Determinar si el cambio mejorará el tráfico de la red alámbrica existente.
- Incorporar una red inalámbrica al sistema sin generar conflictos con los recursos existentes, con la finalidad de que en un futuro los cambios en las ubicaciones de las estaciones de trabajo no implique elevación de costos.

1.3 Justificación

La sustitución del equipo se fundamenta en la premisa de que los errores que se están generando actualmente en nuestra red, son ocasionados por que nuestros equipos que controlan el sistema no están a la altura de la demanda que genera el tráfico de la red a la que dan servicio. El equipo a instalar es un ruteador con capacidad de manejar redes LAN y WLAN, para la mejora del tráfico que actualmente provoca saturación y ocasiona entorpecimientos en la red existente, así también se aumentará la confiabilidad en el nivel de filtrado, que es un punto importante para el correcto funcionamiento de las redes de hoy en día.

1.4 Metodología

El servidor proxy instalado actualmente será sustituido por un equipo de ruteo, por lo que se buscarán y analizarán equipos de diferentes marcas. Una vez concluida la búsqueda se determinará la opción que sea más adecuada para la configuración actual de nuestro sistema así como la del presupuesto autorizado. Ya instalado y configurado el equipo de ruteo se retirará el servidor proxy para resolver posibles detalles que se puedan presentar así como comprobar el nivel de confiabilidad del equipo.

Para la implementación de la red inalámbrica (WLAN), se buscará principalmente que su instalación sea mediante el uso del menor número de equipos posible sin sacrificar la cobertura de la red inalámbrica. De los diversos equipos existentes en el mercado que cuenten con interfase para este tipo de redes, se elegirá el más apropiado para nuestra configuración. Una vez instalado el equipo determinaremos mediante el uso de un equipo móvil con interfase inalámbrica si existen problemas de comunicación a corregir, así como comprobar la distancia de cobertura máxima propuesta por el fabricante con la distancia real de operación del equipo seleccionado.

1.5 Alcance del Proyecto

- Las actividades a realizar durante el proyecto se enfocarán en las redes de área local (LAN), así como su interconexión con las redes (WAN) para compartir un enlace de Internet.
- Se evaluará el sistema que se tiene implementado y se cambiarán solamente los recursos claves, procurando no elevar el costo del proyecto.
- La tecnología inalámbrica que se incluya en el proyecto estará regida por los equipos que se coloquen, los cuales deben ser compatibles con la tecnología que se vende en nuestro país.
- Se mencionarán las ventajas y desventajas al momento de utilizar un servidor proxy y un ruteador como interfase entre redes LAN y WAN para nuestra configuración de red instalada.

1.6 Limitaciones del Proyecto

- El estudio se concretará en la red de área local existente en el sitio de trabajo, la cual está limitada a un número de 15 estaciones de trabajo máximo.

- El costo de las mejoras en nuestro sistema no debe ser muy elevado, con el fin de que pueda ser aprobado e implementado en el menor tiempo posible.

- La arquitectura del edificio en donde se encuentra instalado nuestra red puede limitar en gran medida el uso de la red inalámbrica.

CAPITULO 2

COMUNICACION DE DATOS

2.1 Transmisión de Información

Los términos analógico y digital corresponden a continuo y discreto respectivamente. Ambos son utilizados frecuentemente en comunicaciones en por lo menos 3 contextos: datos, señalización y transmisión.

La información Analógica es aquella que toma valores continuos en un intervalo de tiempo dado como es el caso de la voz, que tiene patrones que varían constantemente en intensidad. Cuando nos referimos a información digital hacemos referencia a información que tiene valores discretos, tenemos por ejemplo los números enteros.

En un sistema de comunicaciones la información es propagada de un punto a otro por señales eléctricas. Una señal analógica es una onda electromagnética que varía continuamente y puede ser propagada por una variedad de medios o propagada hacia la atmósfera o espacio. Una señal digital es una secuencia de pulsos de voltaje que pueden ser transmitidos por cables de cobre, como ejemplo tendíamos un nivel de voltaje positivo constante puede representar al 0 binario y un nivel de voltaje negativo

representa al 1 binario. La principal ventaja de la señalización digital es su bajo costo respecto a la señalización analógica, así como su poca susceptibilidad a la interferencia. La desventaja más importante en la señalización digital es la atenuación o reducción de la señal a altas frecuencias, ocasionando posible pérdida de información en la señal propagada.

La información analógica y digital puede ser representada y propagada por señales analógicas o digitales. Generalmente la información analógica está en función del tiempo y ocupa un espectro de frecuencia limitado. Esta información puede ser representada directamente por una señal electromagnética ocupando el mismo espectro. El mejor ejemplo es la información de voz. El espectro estándar para las señales de voz es de 300 a 3400Hz, el teléfono produce una señal electromagnética con el mismo patrón de frecuencia-amplitud por cada señal de entrada en el rango de 300 a 3400Hz que recibe el auricular.

La señal digital puede ser representada en forma analógica utilizando un MODEM (modulador-demodulador). Este equipo convierte las series de pulsos de voltaje en señal analógica gracias a la modulación de una frecuencia portadora. La señal resultante ocupa cierto espectro de frecuencias centrado en la portadora y puede ser propagado por el medio conveniente para esa portadora. En una operación similar a la realizada por un MODEM, la información analógica puede ser representada por señales digitales. El equipo que realiza dicha función para el caso de la voz es el CODEC (codificador-decodificador). El CODEC toma la señal analógica que representa la información de voz y aproxima esa señal en un tren de bits.

Finalmente, la información digital puede ser representa directamente en forma binaria por dos niveles de voltaje. Para mejorar las características de propagación, la información digital es codificada en una o más señales digitales complejas.

Las señales digitales y analógicas pueden ser transmitidas por varios medios, de los cuales se debe elegir el más adecuado. La manera en la que estas señales son tratadas

está en función del sistema de transmisión. La transmisión analógica es la transmisión de señales analógicas sin importar el contenido, las señales pueden representar información analógica o digital. En ambos casos la señal analógica sufrirá atenuaciones que limitarán su longitud de transmisión. Para alcanzar grandes distancias, la transmisión analógica utiliza amplificadores para incrementar la energía de la señal. Desafortunadamente los amplificadores también amplifican el ruido que lleva la señal a amplificar.

La transmisión digital se preocupa por el contenido de la señal, a diferencia de la transmisión analógica. Como se mencionó anteriormente una señal digital puede ser propagada solo a distancias limitadas debido a la atenuación, pero para alcanzar la transmisión de señales digitales a grandes distancias se introducen repetidores al sistema. La función de un repetidor es recibir la señal digital, recobra el patrón de ceros y unos para retransmitir nuevamente la señal.

2.2 Codificación de Información

Como se ha mencionado la información analógica o digital debe ser transformada en una señal apropiada para la transmisión. En el caso de la información digital, diferentes elementos son utilizados para representar el 1 binario y el 0 binario. El mapeo de los dígitos binarios a elementos de señal es el sistema de codificación usado para la transmisión. Para entender el significado de la codificación se deben considerar 2 tareas principales, la primera es que el receptor debe diferenciar cuando inicia o termina un bit y la segunda es que el receptor debe reconocer el valor de cada bit. Existen diferentes técnicas de codificación para la información analógica y digital, en nuestro caso nos enfocaremos a las técnicas para codificar información digital en forma digital, denominados códigos de línea.

La forma más simple y común es la transmisión de señales digitales utilizando dos niveles de voltaje diferentes. Generalmente, un voltaje negativo es utilizado para representar el uno binario y un voltaje positivo es usado para el cero binario. Este código es conocido como NRZ-L (No Retoro a Nivel Cero). Este código es utilizado para

conexiones de distancias muy cortas como lo es una conexión entre una computadora personal y un MODEM externo.

Otro código sería el NRZI (No Retorno a Cero, Invertido), este código sigue manteniendo un voltaje durante la duración del pulso. La información es codificada por la presencia o ausencia de transición de señal al comienzo de cada pulso. Una transición (Bajo a Alto o Alto a Bajo) al inicio del pulso denota un 1 binario para ese pulso; la no transición indica un 0 binario. NRZI es un ejemplo de codificación diferencial, en la cual la señal es decodificada por la comparación de la polaridad de los pulsos adyacentes en lugar de la determinación del valor absoluto del pulso. Existen desventajas con el uso de la codificación NRZ, la principal es la diferenciación entre el inicio y fin de un bit. Para entender el problema imaginemos que se envía una cadena larga de 1 o 0 para NRZ-L, la salida sería un voltaje constate por un período de tiempo y bajo estas circunstancias cualquier se puede perder la sincronía entre el transmisor y receptor. También es importante hacer notar que existe una componente de corriente directa (dc) que puede ser positiva o negativa según los pulsos dominantes. Existen alternativas de codificación que resuelven estos problemas, se agrupan con el nombre de bifásicas. Dos de estas técnicas son la Manchester y la Manchester Diferencial que son comunes para las redes de área local (LAN). Todas las técnicas bifásicas requieren de por lo menos una transición por bit y como máximo 2 transiciones, debido a esto la taza de modulación es el doble que NRZ ocasionando que el ancho de banda requerido sea mayor. Para compensar esto, estas técnicas tienen varias ventajas:

- Sincronización: debido a que existe una transición en cada bit, el receptor se puede sincronizar durante esa transición.

- No componente dc: gracias a la transición en cada bit, estos códigos no tiene componente de corriente directa.

- Detección de errores: la ausencia de una transición esperada se puede utilizar como detección de errores.

En el código Manchester, existe una transición a la mitad del pulso, la cual se utiliza como señal de reloj. La representación de un 0 binario está dada por una transición de Alto a Bajo y la representación de un 1 binario por una transición de Bajo a Alto. El código Manchester es utilizado en Ethernet y en varias LAN. El Manchester diferencial representa el 0 binario por la presencia de una transición al principio del pulso y el 1 binario es representado por la ausencia de esta transición al inicio del pulso. Este código es utilizado en las redes Token Ring. El código Manchester diferencial tiene la ventaja de emplear la codificación diferencial, esto es si existen dos o más 1 binarios consecutivos sus transiciones serán alternadas.

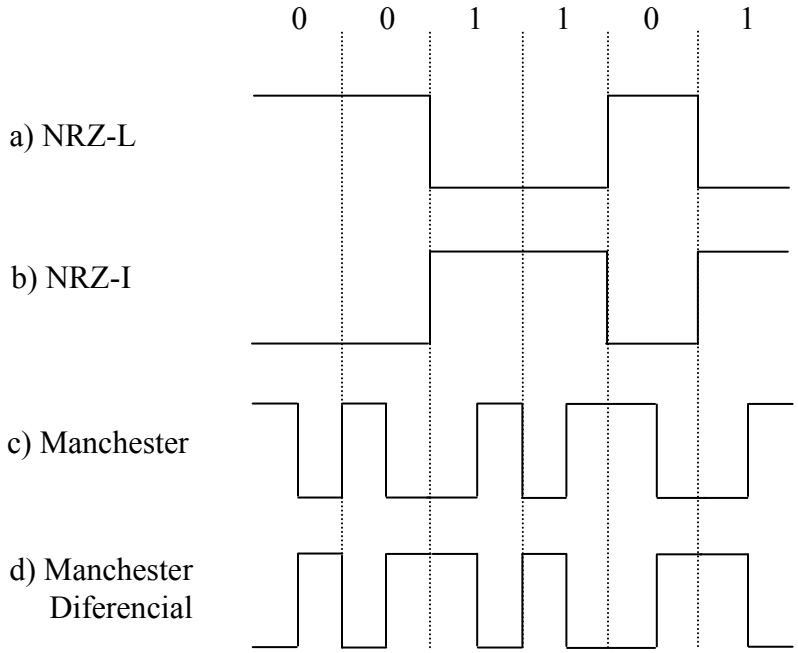


Figura 2.1 Códigos de línea utilizados para codificar la información

2.3 Medios de Transmisión

El transporte de la información de un equipo a otro es posible mediante el uso de medios físicos. Cada uno tiene sus propias características en términos de ancho de banda, retardo, costo y facilidad de instalación y mantenimiento. Los medios se clasifican de forma general en medios guiados (cable de cobre, fibra óptica) y medios no guiados (radio, láser).

2.3.1 Medios Guiados

a) Par Tranzado

Uno de los medios de transmisión más viejos, y aún el más común, es el cable par trenzado. El cual consiste en dos alambres de cobre aislados, por lo general de 1mm de grueso trenzados en forma helicoidal, emulando una molécula de DNA; esto se hace porque dos alambres paralelos constituyen una antena simple y al trenzar los alambres, las ondas de diferentes vueltas se cancelan y la radiación del cable es menos efectiva.

Este tipo de cables se pueden utilizar para la transmisión analógica como digital. El ancho de banda depende del grosor del cable y la distancia que recorre; en muchos casos pueden obtenerse transmisiones de varios mega bits por segundo en distancias de pocos kilómetros. Gracias a su comportamiento adecuado y bajo costo, este tipo de cable se utiliza ampliamente y es probable que su presencia se alargue aún más.

Hay varios tipos de cableado par trenzado, dos de los cuales son importantes para las redes de computadoras. Los cables Categoría 3, los cuales consisten en 2 alambres aislados que se trenzan de manera delicada. Cuatro de estos pares se agrupan por lo regular en una envoltura de plástico para su protección. Antes de 1988, la mayoría de los edificios de oficina tenían este tipo de cable. A comienzos del mismo año se introdujeron los cables par trenzado Categoría 5, los cuales eran similares a los de categoría 3 pero con más vueltas por centímetro, lo que produce una menor diafonía y una señal de mejor calidad a distancias largas. Esto los hace más adecuados para una comunicación más rápida entre computadoras. Las categorías siguientes son la 6 y 7, que tienen capacidad para manejar señales con anchos de banda de 250 y 600Mhz respectivamente. Los cables categoría 3 y 5 manejan 16 y 100MHz respectivamente). Todos estos tipos de cables son conocidos como Par Trenzado sin Blindaje o simplemente UTP.

a) **b)**

Figura 2.2 Cable Par Trenzado. a) Categoría 3. b) Categoría 5

b) Cable Coaxial

Otro medio de transmisión es el cable coaxial, el cual tiene mejor blindaje que el par trenzado, así que puede abarcar distancias más largas. Existen 2 clases de coaxiales que son los más utilizados, el cable de 50 ohms que se utiliza para la transmisión digital y el cable de 75 ohms utilizado para la transmisión analógica y televisión por cable.

El cable coaxial consiste en un alambre de cobre rígido como núcleo, rodeado por un material aislante. El aislante está forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado. El conductor externo se cubre con una envoltura protectora de plástico.

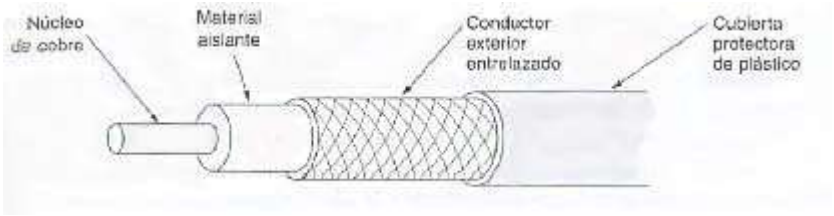


Figura 2.3 Cable Coaxial

La construcción y blindaje del cable coaxial le confieren una buena combinación de ancho de banda y excelente inmunidad al ruido. El ancho de banda posible depende de la calidad y longitud del cable así como la relación señal al ruido de la señal de datos. Los cables modernos tienen un ancho de banda cercano a 1GHz.

c) Fibra Óptica

Los cables de fibra óptica son similares a los coaxiales, excepto por el trenzado. En el centro del cable se encuentra el núcleo de vidrio, a través del cual se propaga la luz. En las fibras multimodo el diámetro es de 50 micras, aproximadamente el grosor de un cabello humano. En las fibras monomodo el núcleo es de 8 a 10 micras.

El núcleo está rodeado por un revestimiento de vidrio con un índice de refracción menor que el núcleo, con el fin de mantener toda la luz en este último. A continuación se

encuentra una cubierta plástica delgada para proteger al revestimiento. Las fibras por lo general se agrupan en haces, protegidas por una funda exterior.

Las fibras se pueden conectar de 3 formas diferentes. La primera de ellas en donde pueden terminar en conectores, los cuales pierden entre 10 y 20% de la luz, pero facilitan la reconfiguración de los sistemas rápidamente. La segunda es el empalme mecánico, los empalmes mecánicos acomodan 2 extremos cortados con cuidado, uno junto a otro, en una manera especial y los sujetan en su lugar. La alineación se puede mejorar pasando luz a través de la unión y haciendo pequeños ajustes para maximizar la señal. La pérdida en estos empalmes es del 10%. La tercera forma existente para conectar las fibras ópticas es mediante la fusión. Los dos extremos de la fibra son fundidos para formar una conexión sólida. Un empalme de fusión es casi tan bueno como una sola fibra, pero aún así hay un poco de atenuación.

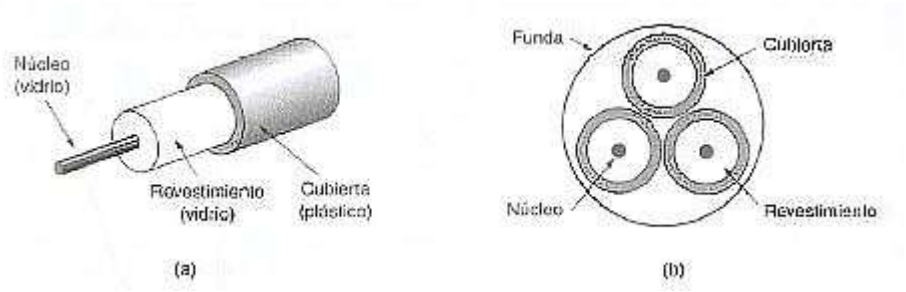


Figura 2.4 Fibra Óptica

Por lo general se utilizan 2 clases de fuentes de luz para producir las señales: LED (Diodos Emisores de Luz) y láser semiconductor. Ambas fuentes tienen propiedades diferentes. En el lado del receptor se encuentra un fotodiodo, el cual emite un pulso eléctrico cuando golpea la luz. El tiempo de respuesta típico de un fotodiodo es 1ns (nanosegundo), lo que limita las tasas de datos a un aproximado de 1Gbps. El ruido térmico también es un problema, por lo que un pulso de luz debe llevar suficiente potencia para que se pueda detectar.

2.3.2 Medios No Guiados

a) Radiofrecuencia

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, y por ello su uso está muy generalizado en la comunicación, tanto en interiores como en exteriores. Estas ondas son omnidireccionales, esto es que viajan en todas direcciones obteniendo como ventaja que el receptor no se tiene que alinear físicamente con el transmisor.

Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias estas ondas cruzan bien casi cualquier obstáculo, pero la potencia se reduce de manera drástica a medida que se aleja de la fuente, aproximadamente en proporción a $1/r^2$ en el aire. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos, incluso son absorbidas por la lluvia. Las ondas de radio en todas las frecuencias, están sujetas a interferencia por motores y equipos eléctricos.

En las bandas VLF, LF y MF las ondas de radio siguen la curvatura de la Tierra, estas ondas se pueden detectar quizá a 1000Km en las frecuencias más bajas, y a menor distancia en frecuencias más altas. En la banda MF se encuentra la radio AM. Este tipo de ondas pueden cruzar con facilidad los edificios, y es por ello que los radios portátiles funcionan en interiores.

En las bandas HF y VHF, las ondas a nivel del suelo tienden a ser absorbidas por la tierra. Sin embargo las ondas que alcanzan la ionosfera (capa localizada a una altura de 100 a 500Km sobre la superficie terrestre) se refractan y se envían de regreso a nuestro planeta. Los operadores de radio aficionados usan estas bandas para conversar a larga distancia.

b) Ondas Infrarrojas y Milimétricas

Este tipo de ondas no guiadas se utilizan mucho para la comunicación de corto alcance. Todos los controles remotos de los equipos eléctricos como lo son televisores, videograbadoras y estéreos utilizan comunicación infrarroja. Estos controles tienen un

inconveniente “no atraviesan objetos sólidos”. Conforme pasamos de la radio de onda larga hacia la luz visible, las ondas se comportan cada vez más como la luz y cada vez menos como la radio. El hecho de que las ondas infrarrojas no atraviesen bien las paredes sólidas también es una ventaja, debido a que en un sistema infrarrojo que se encuentre en un cuarto no interferirá con un sistema similar en cuartos adyacentes.

2.4 Las Interfases de Comunicaciones de Datos

Para que dos equipos que están unidos por un medio de transmisión puedan intercambiar información, se requiere un alto grado de cooperación. Generalmente, la información es transmitida un bit a la vez sobre el medio de transmisión y el tiempo (taza, duración, espaciamiento) de estos bits debe ser el mismo para el receptor como para el transmisor. Existen dos técnicas para controlar este tiempo, el asíncrono y el síncrono.

2.4.1 Transmisión Asíncrona

La transmisión asíncrona para evitar el problema de tiempo, no se envían cadenas largas de bits sin interrupciones y por tal motivo la información es enviada un caracter a la vez, en donde cada caracter tiene cinco u ocho bits de longitud. El tiempo o la sincronización está incluida en cada caracter, por lo que el receptor tiene la oportunidad de sincronizarse al principio de cada nuevo caracter. Cuando no se transmiten caracteres, la línea entre el transmisor y el receptor está en estado reposo. La definición de reposo es equivalente a la señalización para un 1 binario. Así para la señalización NRZ-L, la cual es común para la transmisión asíncrona, el reposo tendrá un voltaje negativo en la línea. El inicio de un caracter es señalizado con un bit de inicio con valor de 0 binario, seguido de los cinco u ocho bits que forman el caracter. Los bits que conforman el caracter son transmitidos iniciando con el bit menos significativo usualmente seguido por un bit de paridad, el cual está en la posición más significante. El bit de paridad es fijado por el transmisor de tal forma que el número total de unos del caracter sea para o impar dependiendo.

Este bit es utilizado por el receptor para la detección de errores. El elemento final es el paro, que es un 1 binario cuya longitud se encuentra ente 1, 1.5 o 2 veces la duración de un bit ordinario. Debido a que el paro y el estado de reposo son iguales, el transmisor enviará la señal de paro hasta que esté listo para enviar el siguiente caracter.

2.4.2 Transmisión Síncrona

En la transmisión síncrona un bloque de bits es transmitido en una cadena fija sin códigos de inicio y paro. El bloque puede tener una longitud de varios bits y para evitar la perdida de sincronía entre transmisor y receptor, sus relojes deben ser sincronizados de alguna forma. Una opción es la posibilidad de enviar una línea de sincronía entre ambos extremos en la cual un extremo pulsa la línea regularmente con un pulso corto y el otro extremo utiliza el pulso como reloj. Esta técnica funciona bien para cortas distancias, pero a distancias mayores el bit de reloj puede sufrir errores. La otra alternativa es incluir la información de reloj en la señal de información; para señales digitales, esto puede ser logrado con la codificación Manchester o Manchester Diferencial.

Con este tipo de transmisión existe otro nivel de sincronización requerido para permitir que el receptor pueda determinar el principio y fin de un bloque de información, para lograrlo cada bloque inicia con un patrón de bit y generalmente termina con otro patrón de bit. Además se agregan otros bits para conducir la información de control. La información mas los patrones de inicio y fin así como el control de información conforman la Trama.

2.4.3 Topología

La topología de un enlace de datos se refiere al arreglo físico de las estaciones en el medio de transmisión. Si solos son dos estaciones el enlace es punto-punto. Si hay más de dos estaciones el enlace es punto multipunto. Tradicionalmente un enlace multipunto ha sido utilizado en el caso de una computadora y varias terminales. Actualmente la topología multipunto se encuentra en las redes de área local.

2.4.4 Full Duplex y Half Duplex

El intercambio de información sobre las líneas de transmisión puede ser clasificada como Half-duplex si solo una de las estaciones en un enlace punto-punto puede transmitir a la vez. Este modelo es conocido como doble vía alternada, el cual sugiere el hecho de que las estaciones se deben alternar para poder transmitir.

En la transmisión Full-duplex, las dos estaciones pueden enviar y recibir información simultáneamente. Este modelo se le conoce como doble vía simultánea. Para el intercambio de información entre dos computadoras full-duplex es más eficiente. Con la señalización digital, que requiere transmisión guiada, full-duplex requiere dos caminos separados de transmisión, en cambio half-duplex solamente requiere uno. Para la señalización analógica, el modo depende de la frecuencia; si la estación utiliza la misma frecuencia para transmitir y recibir solo puede operar en half-duplex para la transmisión inalámbrica y operar en full-duplex para la transmisión guiada utilizando 2 líneas de transmisión separadas. Si la estación utiliza frecuencias diferentes para la transmisión y recepción puede operar en full-duplex para la transmisión inalámbrica y en full-duplex para la transmisión guiada utilizando una línea de transmisión.

2.5 Control de Enlace de Datos

Para que la comunicación digital sea efectiva, se requiere mucho más control para manejar el intercambio. Para lograr el control necesario, una capa lógica es agregada a la interfase física. Esta capa lógica es conocida como control de enlace de datos o protocolo de control de enlace de datos. Cuando un protocolo de control de enlace de datos es utilizado, el medio de transmisión entre sistemas es conocido como enlace de datos.

Para apreciar la necesidad de control de datos, listamos algunos de los requerimientos y objetivos para la comunicación efectiva entre dos estaciones conectadas directamente.

- Sincronización de la Trama: la información es enviada en bloques llamados tramas. El inicio y final de cada trama debe ser reconocible.

- Control de Flujo: la estación transmisora no debe enviar tramas a una velocidad tal que el receptor no pueda recibirlas.
- Control de Error: cualquier bit erróneo introducido por el sistema de transmisión debe ser corregido.
- Direccionamiento: en una línea multipunto, como en las redes de área local, la identidad de las estaciones involucradas en la transmisión deben ser especificadas.
- Control e información sobre el mismo enlace: usualmente es indeseable tener caminos separados para el control de información. El receptor debe de reconocer la información de control de la información que se desea transmitir.
- Manejo del enlace: el inicio, mantenimiento y término de un intercambio de información requiere una cantidad de coordinación y cooperación entre estaciones.

2.5.1 Control de Flujo

El control de flujo es una técnica para asegurar que un equipo transmisor no sature con información al receptor. El equipo receptor usualmente tiene una memoria y cuando la información es recibida, el receptor debe realizar una serie de procesos antes de pasar la información al siguiente nivel. Si se carece de control de flujo, la memoria del receptor se saturaría y desbordaría al momento de estar procesado información previa enviada por el transmisor.

a.- Control de Flujo de Paro y Espera

Es la forma más simple de control de flujo, el cual trabaja de la siguiente forma. Una fuente transmite una trama y el receptor después de aceptar la trama envía un mensaje de control (acknowledgement) para hacer saber al transmisor que está preparado para la recepción de otra trama. El transmisor tiene que esperar hasta recibir la confirmación, la cual indica que se recibió la trama anterior correctamente y se puede enviar la siguiente trama, tal y como se puede apreciar en la figura 2.5a.

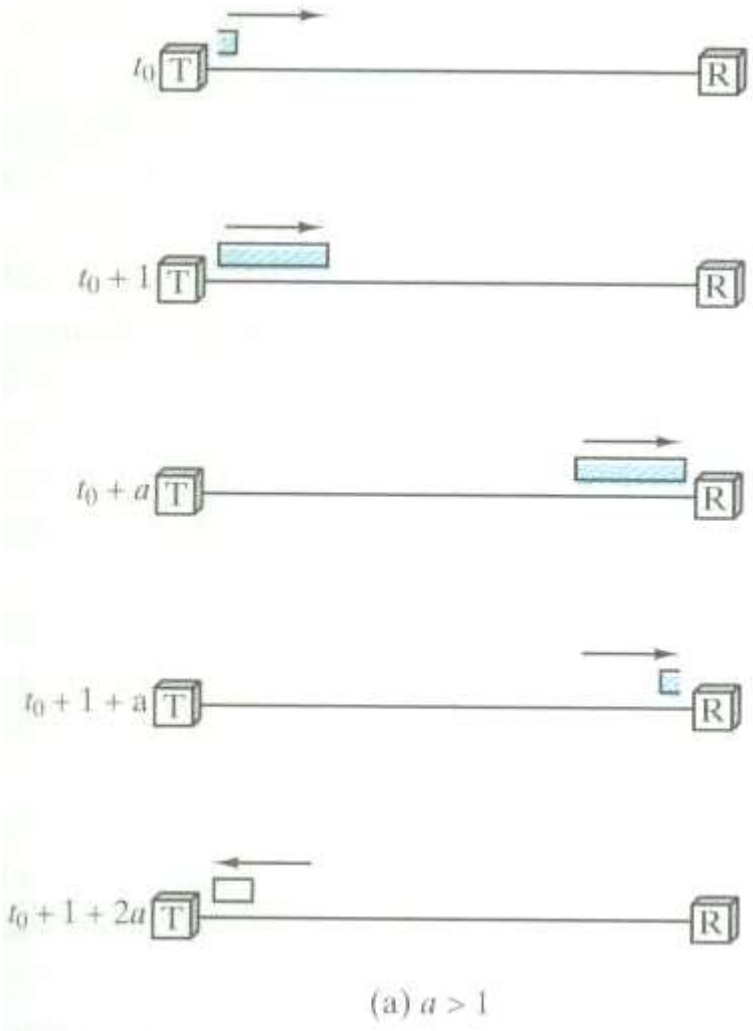


Figura 2.5a Control de Flujo de Paro y Espera

b.- Control de Flujo de Ventana Corrediza

En el control de flujo anterior solamente una trama puede ser transmitida a la vez, por tal motivo no se está utilizando el medio de transmisión eficientemente. Con el control de flujo de ventana podemos transmitir varias tramas a la vez y después recibir la trama de control (acknowledgement). Para una secuencia numérica de k-bits, que provee un rango de secuencia numérica 2^k, el máximo tamaño de la ventana está limitado a $2^k - 1$. Utilizando la figura 2.5b ejemplificaremos el funcionamiento de este control de flujo. Se asume un campo de 3 bits de secuencia numérica y un máximo de 7 tramas para la ventana ($2^3 - 1 = 8 - 1 = 7$). Inicialmente tenemos que A y B tienen ventanas que nos indican que A puede transmitir siete tramas comenzando con la trama 0 (F0). Después

de haber transmitido 3 tramas (F0, F1 y F2) sin señal de control, A disminuye su ventana a 4 tramas indicando que se pueden transmitir 4 tramas comenzando con la trama 3. B transmite una señal RR (Recepción Lista) 3, indicando que se recibieron las tramas 0, 1 ,2 y se está preparado para recibir la número 3; de hecho se está preparado para recibir siete tramas comenzando con la número 3. Con esta señal A está autorizada para transmitir 7 tramas comenzando con la 3, A comienza a transmitir las tramas 3, 4, 5 y 6. B regresa RR4, hasta el cual permite que A envíe incluyendo el marco F2.

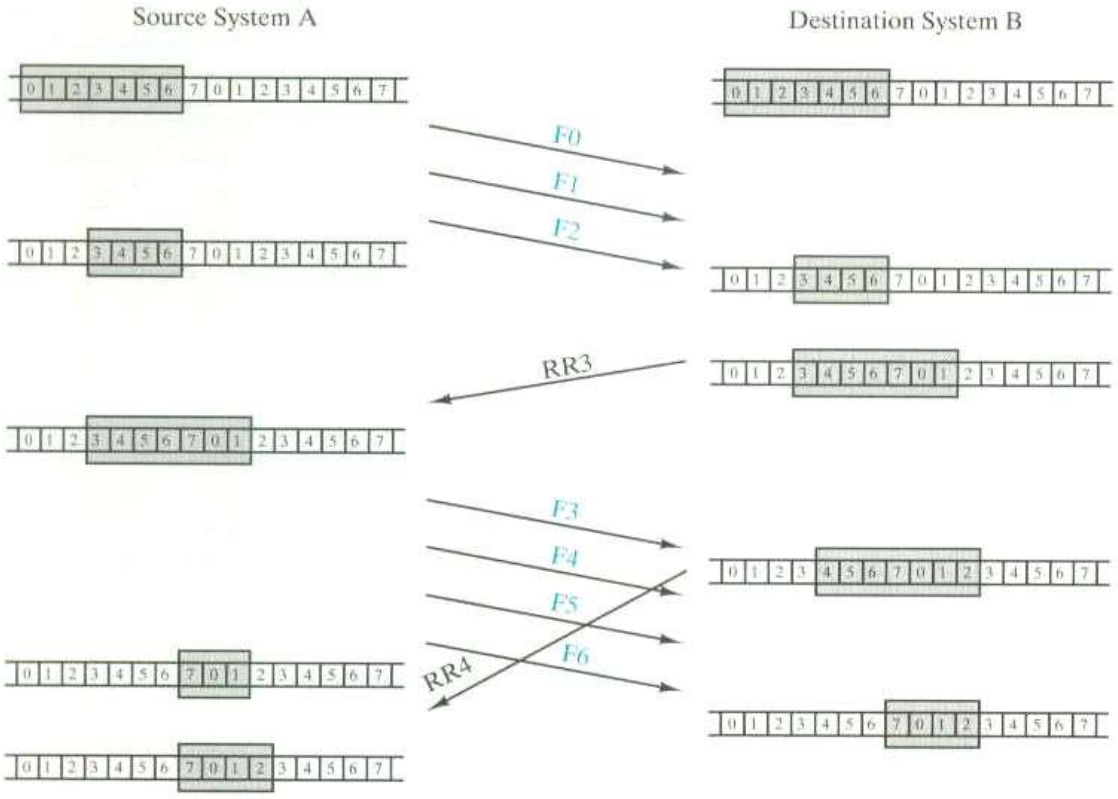


Figura 2.5b Control de Flujo de Ventana Corrediza

El mecanismo descrito no provee una forma de control de flujo, el receptor únicamente debe acomodar 7 tramas desde la última recibida y para hacerlo, la mayoría de los protocolos permiten que las estaciones interrumpan el flujo de tramas enviando un mensaje RNR (No listo para Recibir). Un RNR5 indica que se recibieron todas las tramas hasta la número 4 pero no se puede aceptar la 5 u cualquier otra más. Un tiempo más tarde, la estación envía un mensaje para reabrir la ventana. Es importante mencionar que en los sistemas de 2 vías se requieren 2 ventanas en cada extremo, una para la transmisión y otra para la recepción.

2.5.2 Detección de Errores

Sin importar el diseño de los sistemas de transmisión, siempre habrá errores, resultando en uno o más bits cambiados en la trama transmitida. Definamos estas probabilidades con respecto a errores en las tramas transmitidas:

Probabilidad de un bit de erróneo: conocido también como taza de bit erróneo.

Probabilidad de que la trama llegue sin bits erróneos.

Probabilidad de que la trama llegue con uno o más bits erróneos no detectados.

Probabilidad de que la trama llegue con uno o más bits error detectados pero no se detectan los bit erróneos.

a.- Bit de Paridad

El esquema más simple para la detección de errores es añadiendo un bit de paridad al final del bloque de datos. Tomemos la transmisión ASCII, en la cual se agrega un bit de paridad a cada caracter ASCII de 7 bits. El valor de este bit es seleccionado de tal forma que se tenga un número par de 1s (paridad par) o impar de 1s (paridad impar). En la transmisión síncrona se utiliza paridad par y el la asíncrona impar. Este tipo de esquema no es muy seguro ya que el ruido puede destruir más de un bit.

b.- Código de Redundancia Cíclica

Uno de los códigos de detección de errores más comunes y más potentes son los de comprobación de redundancia cíclica (CRC), que se pueden explicar de la siguiente manera. Dado un bloque o mensaje de k bits, el transmisor genera una secuencia de n bits, denominada secuencia de comprobación de trama (FCS), de tal manera que la trama resultante, con $n + k$ bits, sea divisible por algún número predeterminado. El receptor entonces dividirá la trama recibida por ese número y, si no hay residuo en la división se supone que no ha habido errores.

Utilizaremos la aritmética módulo 2, la cual hace uso de sumas binarias sin acarreo como si se tratara de la operación lógica “or-exlusiva” para aclarar el procedimiento del CRC. Empezaremos con algunas definiciones:

T = Trama de (k+n) bits a transmitir, con n < k.

M = Mensaje de k bits, los primeros k bits de T.

F = n bits del FCS, los últimos n bits de T.

P = Patrón de n+1 bits; este es el divisor elegido.

El objetivo es que la división T/P no genere residuo alguno. Es evidente que

$$T = 2^n M + F$$

El multiplicar M por 2^n, en realidad tiene el efecto de desplazar hacia la izquierda n bits, añadiendo ceros al resultado. Sumar F significa concatenar M y F, y esto no es sino T. El objetivo es hacer T divisible por P. Consideremos el siguiente ejemplo:

1. Dados los siguientes datos:

El mensaje M = 1010001101 (10 bits)

El patrón P = 110101 (6 bits)

La FCS R = de 5 bits

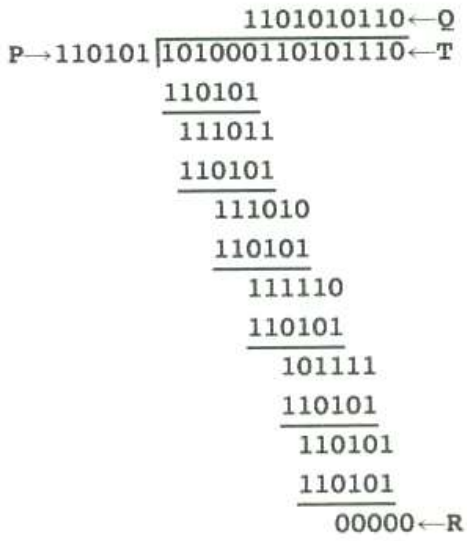
2. El mensaje M se multiplica por 2^5, resultando 101000110100000

3. El resultado anterior se divide por P:

```
                1101010110 ← Q
P → 110101 | 101000110100000 ← 2^n M
             110101
              111011
              110101
                111010
                110101
                  111110
                  110101
                    101100
                    110101
                     110010
                     110101
                        01110 ← R
```

4. El residuo (R = 01110) se suma a 2^nM para dar T = 101000110101110, que es lo que se transmite.

5. Si no hay errores, el receptor recibe T intacto. La trama recibida se divide por P:



Ya que no hay residuo, se supone que no han ocurrido errores. El patrón P se elige con una longitud de un bit más que el FCS deseado, y el patrón elegido en particular depende del tipo de errores que se esperan padecer. Como mínimo, los bits más significativos y menos significativos han de ser 1.

La aparición de un error se puede expresar fácilmente. Un error dará lugar a que un bit se invierta. Esto equivale a calcular la función "or-exclusiva" del bit y 1 (0+1 =1; 1+1=0). Por tanto los errores de una trama de (n+k) bits se pueden representar mediante una palabra de (n+k) bits, teniendo un 1 en aquellas posiciones que coincidan con un error.

2.5.3 Control de Error

Se refiere al mecanismo para detectar y corregir errores que ocurren en la transmisión de tramas. Como se explicó anteriormente, la información se envía en una secuencia de tramas, las cuales llegan en el mismo orden en el que fueron enviadas y cada trama transmitida sufre una cantidad de demora variable y arbitraria. Además se admite la posibilidad de dos tipos de error:

- Trama Perdida: la trama no llega a su destino.

- Trama dañada: una trama reconocible llega pero algunos de los bits tienen errores (fueron alterados durante la transmisión).

Las técnicas de control de error más comunes están basadas en todos o algunos de los siguientes aspectos:

- Detección de error
- Confirmación Positiva. El destino regresa una confirmación positiva cuando se tiene una recepción exitosa y tramas sin errores.
- Retransmisión después de la expiración de un intervalo de tiempo. La fuente retransmite la trama que no ha sido reconocida.
- Reconocimiento negativo y retransmisión. El destino regresa un reconocimiento negativo para las tramas en las cuales se encuentra errores. La fuente nuevamente retransmite la trama.

En conjunto, todos los puntos hacen referencia al ARQ (Petición de Repetición Automática). El fin de el ARQ es convertir a un enlace poco confiable en un en lace de datos confiable. Existen tres versiones de ARQ, las cuales se detallarán a continuación.

a.- ARQ de Paro y Espera

Está basado en una técnica de control de flujo de paro y espera mencionada anteriormente. La estación fuente transmite una trama y espera la señal de control (acknowledgment) ACK, no se envía ninguna trama hasta que la señal de control es recibida por el transmisor. Pueden ocurrir dos tipos de errores en esta versión de ARQ, el primero es que la trama llegue al destino dañada; el receptor detecta el daño mediante el uso de la técnica de detección de error y desecha la trama. Para resolver este problema, el transmisor cuenta con un reloj, en el cual se fija un tiempo de espera para la recepción del mensaje procedente del receptor. Si se acabase el tiempo de espera, el transmisor vuelve a enviar la última trama, debido a que no se recibió mensaje de confirmación por parte del receptor. Debe hacerse notar que el transmisor debe de contar con una copia de la última trama enviada para soportar la pérdida de una trama.

El segundo tipo de error sería el daño de la señal de control (acknowledgment). Tomemos el caso en el cual A envía una trama que es recibida correctamente por B y consecuentemente B envía el mensaje de recepción de trama, el mensaje es dañado en el trayecto y A no reconoce el mensaje por tanto el tiempo de espera caduca y A reenvía nuevamente la última trama la cual es aceptada por B como si fuera una nueva trama provocando duplicado de tramas en B. Para evitar esto, las tramas son marcadas con 0 o 1 y el mensaje de confirmación positiva debe ser ACK0 y ACK1 respectivamente.

b.- ARQ de Retroceso N

Basada en el control de error de ventana corrediza, es el control de flujo más utilizado, en donde una estación puede enviar una serie de tramas numeradas secuencialmente. Cuando no hay errores, el receptor envía un mensaje RR (Listo para Recibir). Si se detecta error se envía el mensaje REJ (Rechazo), el receptor descarta la última trama y todas las subsecuentes. Cuando el transmisor recibe un mensaje REJ envía la trama errónea más todas las subsecuentes. Se pueden presentar los errores de:

1).- Trama dañada.

a) A transmite una trama i. B detecta un error y ha recibido con éxito la trama (i-1). B envía REJ i, indicando que la trama i fue rechazada. A recibe REJ y, retransmitirá i y todas las tramas subsecuentes desde que se transmitió i.

b) La trama i se perdió durante el envío. A envía subsecuentemente las tramas (i+1). B recibe la trama (i+1) fuera de orden y envía el REJ i. A debe retransmitir la trama i y todas las subsecuentes tramas.

c) La trama i se perdió durante el envío y A no transmite tramas adicionales inmediatamente. B no recibe tramas y no regresa mensaje RR o REJ. Cuando el tiempo de espera de A termina, transmite una trama RR que incluye un bit conocido como bit P, el cual es establecido como 1. B interpreta la trama RR con el bit P como un comando que debe responderse con un mensaje RR indicando la siguiente trama a recibir. A recibe RR y retransmite la trama i.

2).- Daño en el mensaje RR.

a) B recibe una trama i y envía un mensaje RR(i+1), el cual se pierde en el trayecto. Ya que los mensajes son acumulativos, esto es que A recibirá un mensaje RR subsecuente de una trama subsecuente y esta debe llegar antes que el tiempo de espera asociado con la trama i expire.

b) Si tiempo de espera de A termina, este transmite un comando RR como en el caso 1c. A también establece otro tiempo de espera llamado P-bit. Si B falla en responder al comando RR o si la respuesta se daña, el tiempo P-bit expira. En este punto A intentará nuevamente, enviando un comando RR y reiniciando el tiempo P-bit. Este procedimiento es intentado varias veces. Si A no recibe un mensaje de respuesta luego de varios intentos, se inicia un proceso de reinicio.

3).- El mensaje REJ dañado. Si REJ es perdido, equivale al caso 1c.

c.- ARQ de Repetición Selectiva

En esta variación de ARQ, solamente se retransmiten las tramas de las cuales se recibe un mensaje negativo de recepción, el cual denominaremos SREJ. Esta versión de ARQ parece ser más eficiente que el ARQ de Retroceso N ya que se minimiza la cantidad de retransmisiones. Por otro lado, el receptor debe de contar con una memoria (buffer) lo suficientemente grande para almacenar las tramas que lleguen antes de la transmisión de la trama dañada y también debe tener lógica para reinsertar la trama dañada en la secuencia correcta. El transmisor requiere una lógica compleja para que sea posible el envío de una trama fuera de secuencia. Debido a todas estas complicaciones, el ARQ de repetición selectiva es menos utilizado que el de retroceso N.

2.6 Multiplexión

Generalmente dos estaciones que se comunican no utilizan la capacidad total del enlace de datos y es posible compartir la capacidad del mismo. Un término que se utiliza para esta actividad es la multiplexión. La figura 2.6 muestra la multiplexión en su forma más simple. Existen *n* entradas al multiplexor, el cual está conectado por un solo enlace

de comunicación con el demultiplexor. El enlace deber ser capaz de transportar *n* canales de información separados. El multiplexor combina (multiplexa) la información de las *n* líneas de entrada y las transmite sobre el enlace de alta capacidad. El multiplexor acepta la cadena de datos multiplexada, separa (demultiplexa) la información de acuerdo al canal y la entrega a las líneas de salida correspondientes.

Figura 2.6 Ejemplo de Multiplexión

2.6.1 Multiplexión por División de Frecuencia

La multiplexión por división de frecuencia es posible cuando el ancho de banda útil en el medio de transmisión excede el ancho de banda requerido por las señales a ser transmitidas. Un número de señales puede ser transmitida simultáneamente si cada señal es modulada en una frecuencia portadora diferente y las frecuencias portadoras está suficientemente separadas de tal forma que el ancho de banda de las señales no se empalmen. Un caso general de FDM se aprecia en la figura 2.7, en donde seis fuentes de señal son introducidas al multiplexor, quien modula cada señal en una frecuencia diferente ($f_1 \ldots f_6$). Cada señal modulada requiere un cierto ancho de banda centrado en la frecuencia portadora, esto se entiende como canal. Para prevenir interferencias, los canales son separados por unas guardas, las cuales son porciones de espectro sin utilizar.

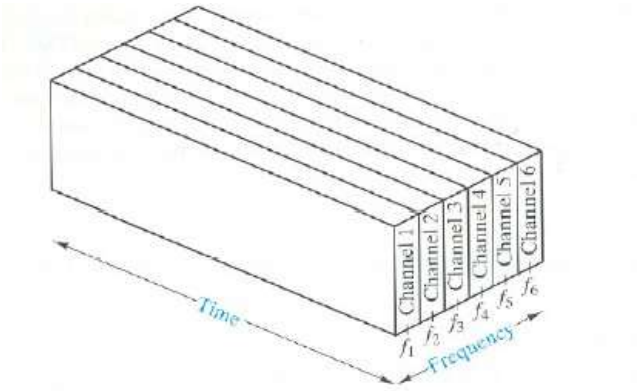
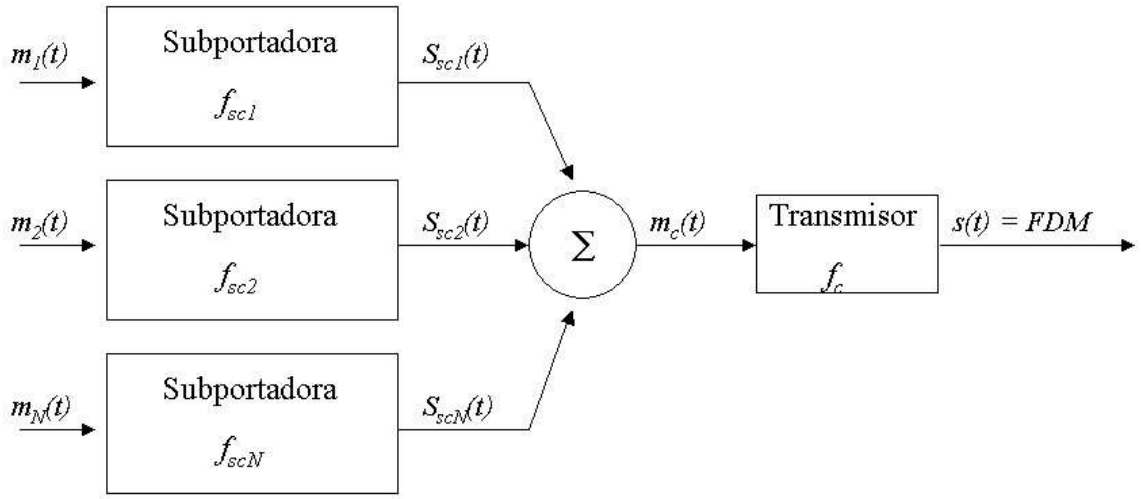


Figura 2.7 Multiplexión por División de Frecuencia (FDM)

La señal compuesta transmitida por el medio es analógica, sin importar si las señales de entrada del multiplexor son analógicas o digitales. En el caso de las señales digitales, las señales de entrada deben ser convertidas a señales analógicas mediante el uso de modems.



a) Transmisor

Figura 2.8 Ejemplo de un transmisor para FDM

Una descripción general de FDM se encuentra en la figura 2.8. Un número de señales analógicas o digitales [$m_i(t)$, $i = 1, N$] serán multiplexadas sobre el mismo medio de transmisión. Cada señal $m_i(t)$ es modulada sobre una portadora f_{sci}, debido a que múltiples portadoras serán utilizadas, cada una es referida como subportadora. Cualquier tipo de modulación se puede utilizar. Las señales moduladas analógicas resultantes son sumadas para producir la señal compuesta $m_c(t)$. La figura 2.9 muestra el resultado. El espectro de la señal $m_i(t)$ es movido para estar centrado en f_{sci}. Para que este esquema trabaje se debe elegir una f_{sci} de tal forma que los anchos de banda de varias señales no se traslapen, ya que de ocurrir un traspale sería imposible recuperar la señal original

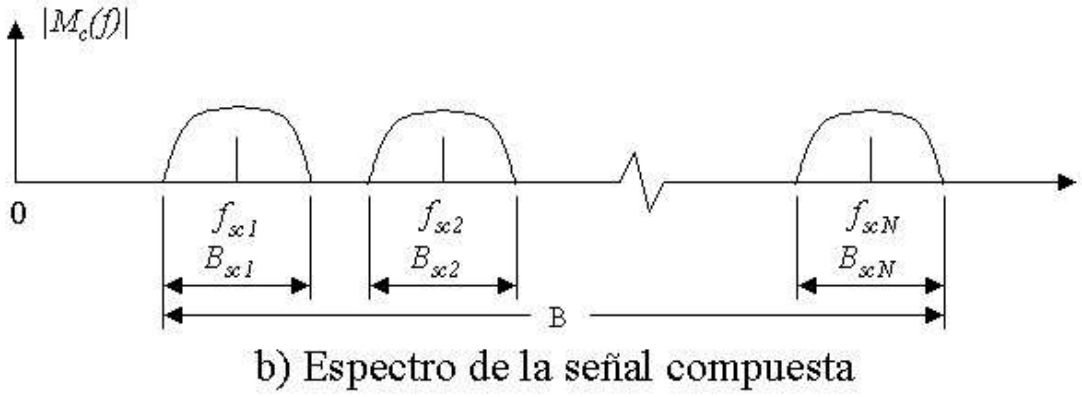


Figura 2.9 Ejemplo del espectro de la señal en FDM

La seña compuesta puede ahora ser manejada como un todo hacia otra frecuencia portadora para una modulación adicional. Esta segunda modulación no utiliza la misma modulación que la utilizada anteriormente. La señal compuesta tiene un ancho de banda total B, donde $B > \sum_{i=1}^{N} B_{sci}$. Esta señal analógica puede ser transmitida sobre el medio adecuado. En la parte del receptor, la señal compuesta es pasado a través de *N* filtros pasabanda, cada uno de los cuales está centrado en f_{sci} y tienen una ancho de banda B_{sci} para $1 < i < N$; de esta forma la señal es dividida en sus componentes . Cada componente es luego demodulado para recuperar la señal original como se aprecia en la figura 2.10.

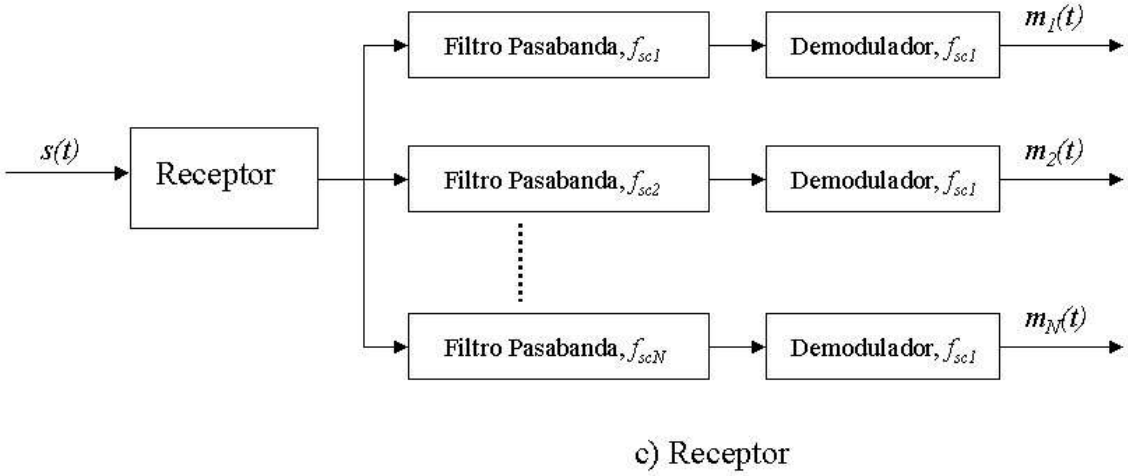


Figura 2.10 Ejemplo de un receptor para FDM

2.6.2 Multiplexión por División de Tiempo

Este tipo de multiplexión es posible cuando la taza de transferencia del medio excede la taza de transferencia de las señales digitales a ser transmitidas. Señales digitales múltiples pueden ser transportadas sobre una línea de transmisión, mediante la interpolación de cada señal en el tiempo. Como se puede apreciar en la figura 2.11, se tienen 6 entradas de 9.6kbps y una línea con una capacidad de 57.6kbps en donde se pueden acomodar todos los 6 canales fuente.

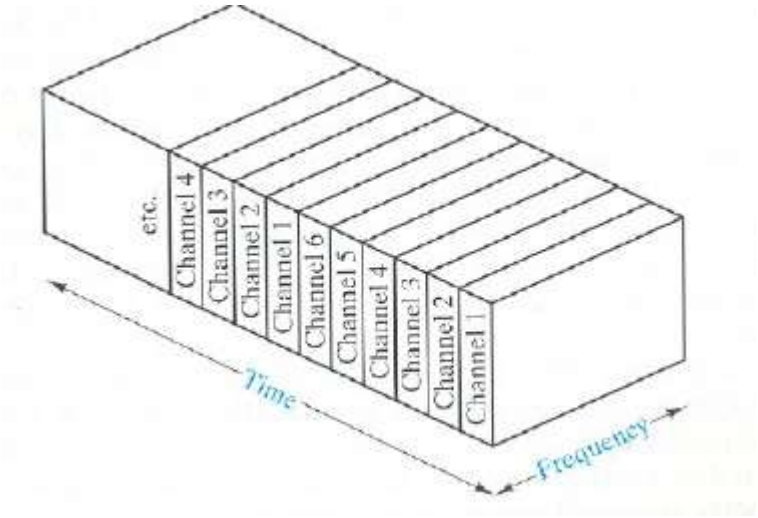


Figura 2.11 Multiplexión por División de Tiempo (TDM)

Utilizando la figura 2.12a en donde un número de señales [$m_i(t)$, i=1, N] serán multiplexadas sobre el mismo medio de transmisión. La señal de entrada de cada fuente es almacenada brevemente en un buffer (memoria). Cada buffer tiene una longitud típica de un bit o un caracter. Los buffers son barridos secuencialmente para formar un flujo digital de datos $m_c(t)$. El escaneo o barrido es lo suficientemente rápido de tal forma que el buffer o memoria es vaciado antes de que llegue nueva información al mismo, por tal motivo la velocidad de $m_c(t)$ debe ser al menos igual a la suma de las velocidades de $m_i(t)$. La señal digital $m_c(t)$ puede ser transmitida directamente o puede ser ingresada a un modem para obtener una señal analógica y posteriormente transmitir esta señal. La señal transmitida puede tener un formato parecido al mostrado en la figura 2.12b.

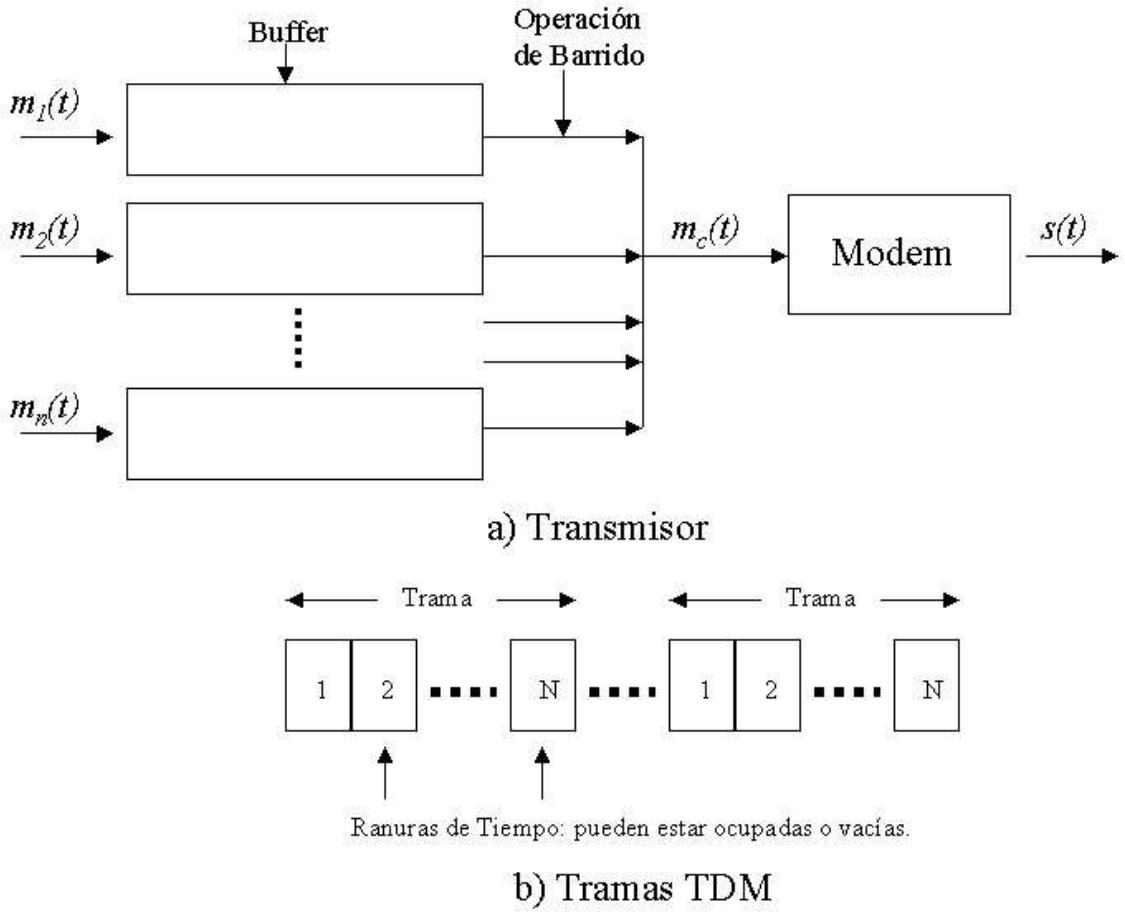


Figura 2.12 Ejemplos de un modelo TDM. a) Transmisor. b) Trama TDM

La información es organizada en tramas, las cuales contienen un ciclo de las ranuras de tiempo. En cada trama una o más ranuras son dedicadas a cada fuente de datos. La secuencia de las ranuras dedicadas a una fuente se le denomina canal. La longitud de la ranura de tiempo es igual a la longitud del buffer de transmisión, comúnmente de un bit o un carácter.

La técnica interpolación de caracteres es utilizada con fuentes asíncronas. Cada ranura de tiempo contiene un carácter de información. Comúnmente los bits de inicio y fin de cada carácter son eliminados antes de la transmisión y reinsertados por el receptor. La técnica de interpolación de bit se utiliza con las fuentes síncronas, aunque también

puede ser utilizada con las asíncronas. Cada ranura de tiempo contiene un bit de información.

En el receptor, la información interpolada es demultiplexada y llevada al buffer de destino apropiado. Para cada fuente $m_i(t)$ hay una salida idéntica que recibe la información de entrada a la misma velocidad en la que fue generada.

Es posible que con equipos TDM se manejen fuentes de distintas tazas de transferencia. Por ejemplo, a la entrada con menor taza de transferencia se le puede asignar una ranura por ciclo, mientras que a la entrada con mayor taza se le asignen múltiples ranuras por ciclo.

CAPITULO 3

REDES DE AREA EXTENDIDA

Las redes de área extendida (WAN), abarcan una gran área geográfica, con frecuencia un país o un continente. Contienen un conjunto de máquinas diseñado para aplicaciones de usuario, quienes están conectados por una subred de comunicación. La función de una subred es llevar los mensajes de un usuario a otro, como lo hace el sistema telefónico con las palabras del que habla al que escucha. La separación de los aspectos de la comunicación pura de la red de los paquetes de aplicación, simplifica en gran medida todo el diseño de la red.

En la mayoría de las redes de área amplia la subred consta de dos componentes distintos: las líneas de transmisión y elementos de conmutación. Las primeras mueven los bits entre máquinas y pueden estar hechas de cobre, fibra óptica o enlaces de radio. Los elementos de conmutación son computadoras especializadas para conectar tres o más líneas de transmisión. Cuando los datos llegan a una línea de entrada, el elemento de conmutación debe elegir una línea de salida en la cual reenviarlos. Estas computadoras de conmutación reciben nombres como conmutadores o rutadores.

3.1 Conmutación de Circuitos

Para la transmisión de información fuera de un área local, la comunicación se logra transmitiendo la información de la fuente a su destino a través de una red de conmutada de nodos; esta red conmutada es en ocasiones utilizada para implementar redes LAN y MAN. Los nodos conmutados no les importa el contenido de la información, ya que su propósito es proveer una conmutación que ayude a mover la información de nodo a nodo hasta alcanzar su destino. Los equipos finales que desean comunicarse se les conoce como estaciones y pueden ser computadoras, teléfonos, terminales u otros equipos de comunicaciones. Los equipos que proporcionan la conmutación se les denomina nodos, los cuales están conectados unos con otros mediante una topología por líneas de transmisión. Cada estación conectada a un nodo y al conjunto de nodos se les conoce como red de comunicaciones.

La comunicación vía conmutación de circuitos implica un camino dedicado para la comunicación de dos puntos. Este camino es una secuencia de conexiones entre nodos. Cada enlace físico tiene un canal dedicado para la conexión. El ejemplo más común es la red telefónica. La comunicación de circuitos abarca tres fases:

- Establecimiento del circuito: antes que la información sea transmitida, se debe establecer un circuito punto a punto. Utilizando la figura 3.1, se desea que la estación A establezca comunicación con la estación E. La estación A solicita al nodo 4 una petición de conexión con E y debido a que la conexión entre A y el nodo 4 es dedicada, esa conexión ya existe. El nodo 4 debe encontrar un camino para alcanzar el nodo 6. Basado en la información de ruteo, disponibilidad y tal vez costo se elige el nodo 5 donde se localiza un canal libre en el circuito. Se envía una petición para la conexión con E. El nodo 5 localiza un canal libre que lo comunique con el nodo 6 y comunica ese canal con el canal existente hacia el nodo 4. El nodo 6 completa la conexión con E. Al completar la conexión se envía una prueba para determinar si E está ocupado o libre para aceptar la conexión.

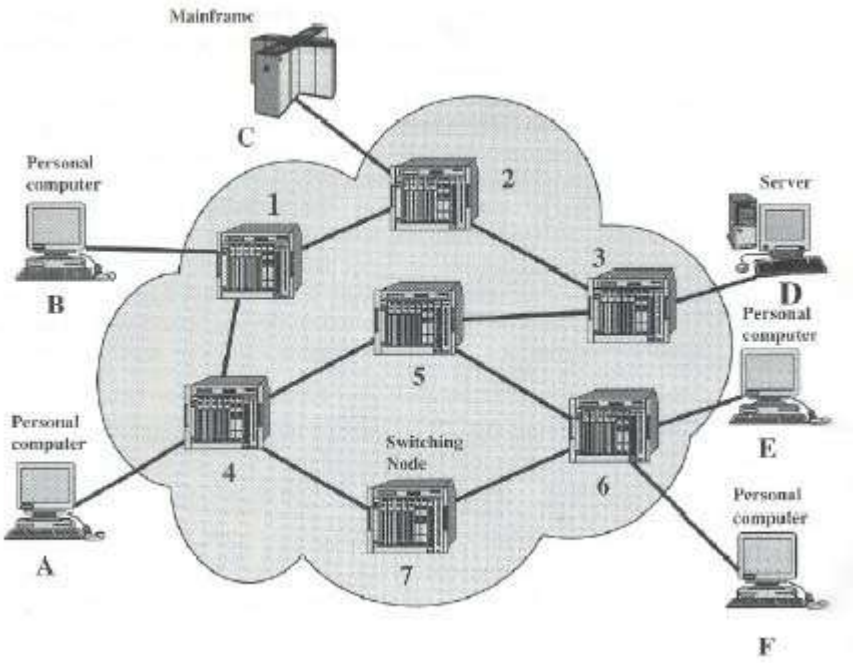


Figura 3.1 Ejemplo de una red simple de conmutada de circuitos

- Transferencia de Información: las señales pueden ser transmitidas de A hasta E una vez que se estableció el circuito de comunicación. Generalmente la conexión es Full Duplex, esto es que la información puede ser transmitida en ambas direcciones al mismo tiempo.

- Desconexión del circuito: después de un determinado tiempo, la conexión es terminada usualmente debido a una de las dos estaciones. Las señales de terminación deben ser enviadas a los nodos 4, 5 y 6 para que liberen los recursos dedicados a la comunicación.

Es importante hacer notar que se requiere un camino de conexión antes de enviar cualquier información, de manera que el canal debe estar reservado y disponible para la conexión entre los nodos de la red. La conmutación de circuitos puede ser ineficiente, debido a que la capacidad del canal está dedicada por el tiempo que dure la conexión sin importar si se está transmitiendo o no información. Sin embargo, una vez establecido el circuito de comunicación, la red es transparente para los usuarios.

3.2 Conmutación de Paquetes

En la conmutación de paquetes, la información es transmitida en bloques llamados paquetes. Tenemos un límite típico para los paquetes que es de 1000 octetos (bytes). Si la fuente tiene un mensaje más grande para enviar, el mensaje es divido en una serie de paquetes antes de ser transmitido. Cada paquete consiste en una porción de información más un cabecero que contiene información de control. La información de control incluye mínimo la información que requiere saber el dispositivo de red para que el paquete sea entregado a su destino. En cada nodo de la ruta, el paquete es recibido y almacenado un corto tiempo para después enviarlo al siguiente nodo. Dentro de las ventajas de la conmutación de paquetes con respecto a la conmutación de circuitos encontramos las siguientes:

- La eficiencia de la línea es mayor, un enlace nodo a nodo puede ser dinámicamente compartidos por varios paquetes al mismo tiempo. Los paquetes son preparados y transmitidos por el enlace tan rápido como sea posible.

- En una red de conmutación de paquetes puede realizar conversión de razón de transferencia. Dos estaciones con diferentes razones de transferencia pueden intercambiar paquetes, debido a que cada nodo se conecta a su propia razón de transferencia.

- Cuando el trafico es mucho en una red de circuitos conmutados, algunas llamadas son bloqueadas; esto es que la red se niega a aceptar peticiones de conexión adicionales hasta que la carga de la red se reduzca. En una red de conmutación de paquetes, los paquetes son aceptados pero el tiempo entrega se alarga.

- Se puede utilizar prioridades. De esta forma si un nodo tiene un número de paquetes listos para transmitir, éste pude transmitir primero los paquetes de alta prioridad. Estos paquetes experimentarán un retardo menor que los de baja prioridad

Expliquemos el funcionamiento de la red de conmutación de paquetes. Considere que se desea enviar un mensaje que excede el tamaño del paquete máximo, por tal motivo el mensaje original es dividido en paquetes que serán enviados por la red. Una pregunta que se podrían presentar es el cómo la red manejará este conjunto de paquetes en su intento de rutearlos por la red y entregarlos al destinatario. Existen 2 opciones: Datagrama y Circuito Virtual.

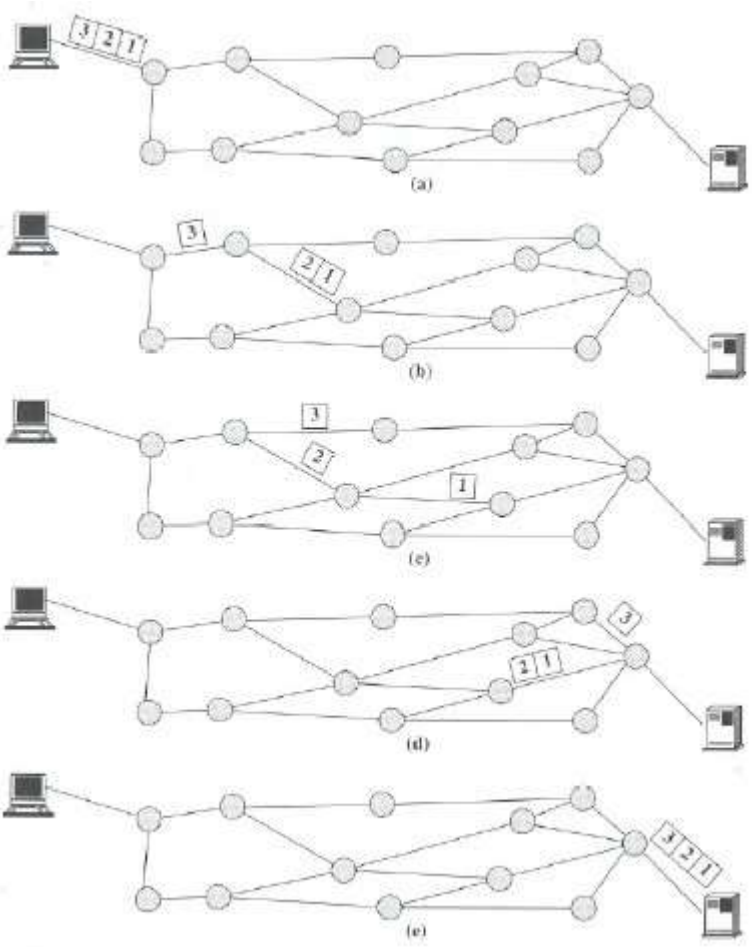


Figura 3.2 Trayectoria de paquetes de información utilizando Datagramas.

En un datagrama, cada paquete es tratado independientemente sin referencia a paquetes que se hallan enviado anteriormente. Cada nodo elige el siguiente nodo en la ruta del paquete, tomando en cuenta información como tráfico, estado de las líneas y más de nodos vecinos. De esta forma los paquetes, aún con el mismo destino, no siempre siguen el mismo camino y pueden llegar fuera de secuencia al punto de salida.

En el ejemplo, el nodo de salida acomoda los paquetes a su orden original antes de entregarlos al destino final. En algunos datagramas, esta tarea es realizada en el destino en lugar del nodo final. También es posible que un paquete sea destruido en la red. Por ejemplo, si un nodo falla momentáneamente todos los paquetes que tenga almacenados se perderán. Nuevamente es tarea del nodo final o del destino el detectar la pérdida del paquete y decidir cómo recuperarlo. En esta técnica, cada paquete es manejado independientemente y referido como un datagrama. Lo anterior lo podemos observar en la figura 3.2

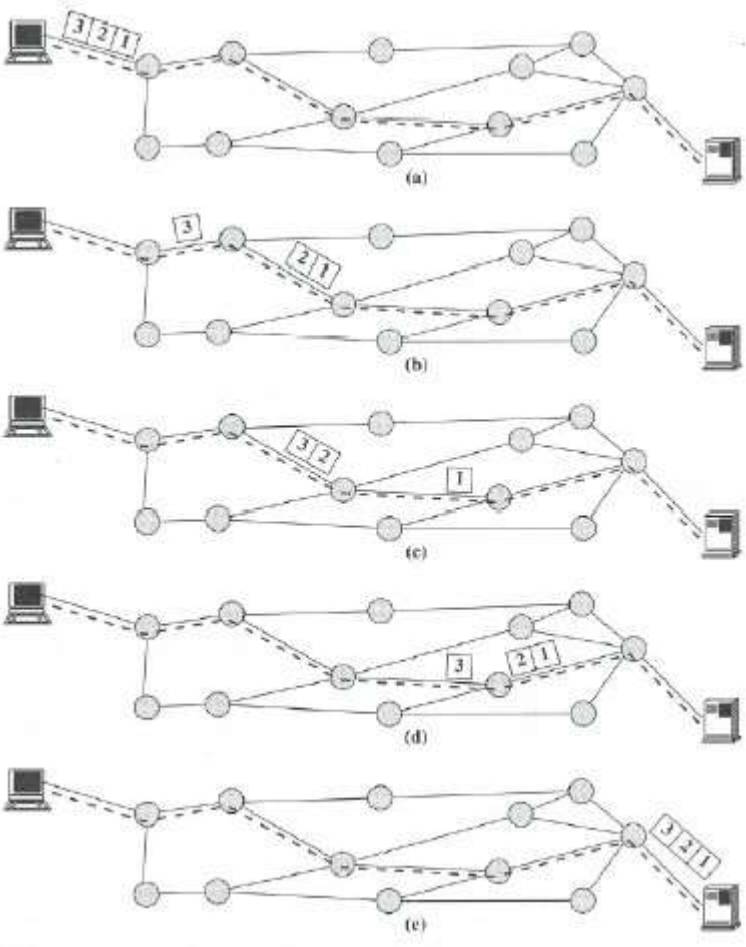


Figura 3.3 Trayecto de paquetes utilizando Circuitos Virtuales

Para el circuito virtual, una ruta preplaneada es establecida antes de que los paquetes sean enviados; esta ruta sirve para mantener la conexión lógica con el destino final. Una vez que la ruta es establecida, todos los paquetes entre los dos puntos a comunicar

siguen la misma ruta a través de la red. Debido a que se prepara una ruta para la duración de la conexión lógica, es en alguna forma similar a un circuito de una red de circuitos conmutados y es mencionado como circuito virtual. Cada paquete ahora contiene un identificador de circuito virtual e información del mensaje original. Cada nodo en la ruta preestablecida sabe a dónde dirigir estos paquetes; no se requieren decisiones de ruteo. En cualquier momento cada estación puede tener más de un circuito virtual para otra estación. De tal forma, la principal característica de la técnica de circuito virtual es que la ruta entre las estaciones es establecida antes de la transferencia de información. Note que la ruta no es un camino dedicado como en la conmutación de circuitos. Un paquete aún es almacenado en cada nodo y preparado para salir por una línea, pero la diferencia con el datagrama es que con circuitos virtuales el nodo no requiere de tomar decisiones de ruteo para cada paquete (Figura 3.3). La decisión es tomada una sola vez para todos los paquetes cuando utilizamos circuitos virtuales.

3.3 Frame Relay

En la década de 1980 aparece Frame Relay, red que está orientada a la conexión sin control de errores ni de flujo. Debido a que es una red orientada a la conexión los paquetes son entregados en orden. Estas propiedades la hicieron parecida a una red LAN de área extendida. Su aplicación más importante es la interconexión de LANs en múltiples oficinas de una empresa sobre redes públicas o privadas. Frame Relay es una interfaz de usuario dentro de una red de conmutación de paquetes de área extensa, que típicamente ofrece un ancho de banda en el rango de 56 Kbps y 1.544 Mbps. Frame Relay se originó a partir de las interfaces ISND y se propuso como estándar en 1984.

Un circuito virtual permanente (PVC) consiste en un trayecto predefinido a través de la red Frame Relay que conecta dos puntos finales. El servicio Frame Relay proporciona PVCs situados donde hayan especificado los clientes, entre los emplazamientos designados. Estos canales permanecen activos continuamente y están garantizados, con objeto de proporcionar un nivel específico de servicio. Los circuitos virtuales

conmutados se añadieron al estándar Frame Relay a finales de 1993, así Frame Relay se ha convertido en una auténtica red de conmutación "rápida" de paquetes.

Como las redes locales generan flujos esporádicos, el consumo de ancho de banda debe adaptarse a sus necesidades particulares y aquí reside precisamente la ventaja esencial de Frame Relay que ajusta el ancho de banda a las aplicaciones con pequeños tiempos de tránsito. Además, cuenta con otras ventajas técnicas como su velocidad de transmisión (64Kbps y 2Mbps), flexibilidad de utilización y apertura hacia ATM.

Al haber sido desarrollado mucho después que la tecnología X.25, Frame Relay se adapta mejor a las características de las infraestructuras de telecomunicaciones actuales. La norma está descrita sólo sobre las dos primeras capas o niveles del modelo OSI, a diferencia de X.25, que llega hasta el Nivel 3 de red, en el cual se consignan las funciones de control del flujo y la integridad de los datos. Por tanto, al estar liberado de estos cometidos, Frame Relay resulta mucho más rápido que X.25, que como fue concebida inicialmente para operar con circuitos analógicos utiliza procedimientos de control de errores, frecuentemente pesados, lentos y complejos.

La evolución tecnológica ha logrado mejorar la calidad de las líneas, permitiendo desplazar el control de los errores a los propios equipos situados en los extremos de la comunicación, que pueden interpretar las señales de control de flujos generadas por la red. En todos estos aspectos técnicos reside la fuerza de Frame Relay, que además, permite al usuario pagar sólo por la velocidad media contratada y no sobre el tráfico cursado. La Velocidad Media de Transmisión (CIR) es un parámetro de dimensión de red específico de Frame Relay que permite a cada usuario elegir una velocidad media garantizada en los dos sentidos de la comunicación para cada circuito virtual (CV). Como no todos los circuitos virtuales utilizan en un mismo momento su ancho de banda reservado, un determinado CV puede emitir parte de su carga hacia los otros. Es obvio que esta gestión dinámica del ancho de banda interesa particularmente a los responsables de telecomunicaciones de las empresas, sobre todo a la hora de tratar el tráfico en

ráfagas propia de la interconexión de redes locales. En resumen, Frame Relay permite dividir estadísticamente el ancho de banda entre diferentes circuitos virtuales.

A diferencia de la conmutación de datos X.25, Frame Relay no posee mecanismos de control local del flujo, cuando la congestión aumenta hasta alcanzar niveles considerables, el retraso de la red se incrementa en gran medida. Este inconveniente conlleva, sin embargo, una de las principales ventajas de esta tecnología, ya que agiliza y simplifica la transferencia de las tramas Frame Relay.

CAPITULO 4

REDES DE AREA LOCAL

Las redes de área local o LAN (Local Area Network) como su nombre lo indica son colocadas para enlazar equipos que se encuentran relativamente cerca o espacios limitados como lo sería un edificio o una casa. Estas redes comparten la característica de ser redes de transmisión de paquetes. En este tipo de redes cada estación está unida al medio de transmisión compartido por otras estaciones. En su forma más simple, una transmisión de cualquier estación es enviada y recibida por todas las estaciones.

4.1 Tecnología LAN

Los protocolos definidos específicamente para las transmisiones LAN son independientes de la arquitectura de la red y son aplicables a las LAN y WAN. El modelo de referencia que se utiliza fue desarrollado por la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) y denominado modelo IEEE 802. Este modelo ha sido adoptado por todas las organizaciones que trabajan en la especificación de los estándares LAN. Si iniciamos a trabajar de abajo hacia arriba, la capa inferior del modelo de referencia IEEE 802 corresponde a la capa física del modelo OSI, e incluye funciones como:

- Codificación /Decodificación de señales
- Generación /Retiro de preámbulos (para la sincronización)

- Transmisión /Recepción de Bits

Además, la capa física del modelo 802 incluye especificaciones de los medios de transmisión y la topología. La elección del medio de transmisión y la topología son críticas en un diseño de LAN. Arriba de la capa física existen funciones asociadas con la provisión de servicio a los usuarios de la LAN, estos incluyen:

- En la transmisión, el armado de la trama con dirección y campos de detección de error.
- En la recepción, desarmado de la trama, reconocimiento de dirección y detección de errores.
- Administración del acceso al medio de transmisión de la LAN.
- Proveer una interfase hacia las capas superiores y ejecutar control de error y flujo.

Las funciones antes mencionadas están agrupadas en la Capa de Enlace Lógico (LLC). Las primeras tres funciones son tratadas en una capa separada llamada Control de Acceso al Medio (MAC).

4.1.1 Topologías

Las topologías más comunes para las LAN son bus, árbol, anillo y estrella. La topología bus es un caso especial de la topología árbol, con un solo tronco y ninguna rama y por tal motivo manejaremos estas dos topologías en conjunto.

a) Topología Bus/Árbol

Ambas topologías se caracterizan por utilizar un medio multipunto. En el caso de la topología bus, todas las estaciones están unidas directamente al medio de transmisión o bus mediante la utilización de una interfase apropiada llamada “tap”. La operación Full Duplex entre la estación y el tap permite ala información ser transmitida al bus y recibida del bus. La transmisión de cualquier estación se propaga a lo largo del medio en ambas direcciones y puede ser recibida por todas las estaciones. El final del bus se coloca un terminador que absorbe cualquier señal y la remueve del bus.

La topología de árbol es una generalización de la topología bus. El medio de transmisión es un cable con ramificaciones sin lazos cerrados. La disposición de árbol comienza en el punto conocido como *headend*, en donde inician uno o más cables y cada uno puede tener ramificaciones. Las ramificaciones pueden tener más ramificaciones formando arreglos complejos. Nuevamente la transmisión de un equipo puede ser recibido por todas las estaciones.

Se presentan 2 problemas al utilizar estos arreglos, el primero es que se requiere una indicación para saber a quién desea transmitir la información y el segundo, es la regulación de la transmisión. Para resolver estos problemas, las estaciones transmiten en pequeños bloques conocidos como tramas. Cada trama consiste en una porción de información que se desea transmitir más un encabezado de trama que contiene información de control. Cada estación se le asigna una dirección o identificador único y la dirección de destino es incluida en el encabezado de la trama.

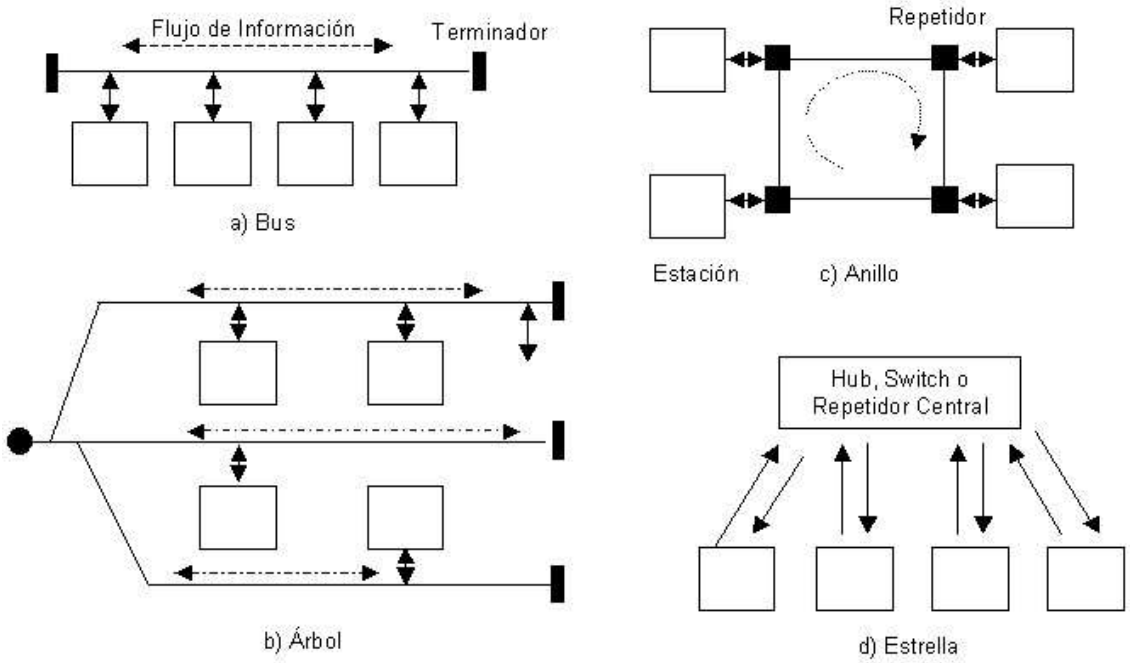


Figura 4.1 Topologías LAN a) Bus. b) Árbol. c) Anillo. d) Estrella

b) Topología Anillo

En esta topología la red consiste en un grupo de repetidores unidos por enlaces punto-punto en lazo cerrado. El repetidor es un equipo simple, capaz de recibir información por un enlace y transmitirlo bit por bit sobre otro enlace tan rápido como se recibe. El repetidor no debe tener memoria. Los enlaces son unidireccionales, es decir que la información es transmitida en una dirección solamente ya sea a favor o en contra de las manecillas del reloj.

Como en la topología bus, la información es transmitida en tramas. Durante la circulación de la trama, ésta pasa por todas las estaciones y la estación de destino reconoce su dirección y copia la trama en una memoria local. La trama continúa circulando en el anillo hasta llegar a la estación fuente en donde es removida del medio. Ya que muchas estaciones comparten el anillo, es requerido un control de acceso al medio para determinar en qué tiempo las estaciones pueden colocar sus tramas.

c) Topología Estrella

En la topología estrella cada estación está directamente conectada a un nodo central común. La conexión de la estación al nodo central se realiza mediante el uso de dos enlaces punto-punto, en donde un enlace es dedicado para la transmisión y otro para la recepción.

En general hay dos alternativas para la operación del nodo central. Una forma es que el nodo central opere en la forma de difusión, en donde la transmisión de la trama de una estación al nodo central es retransmitida a todos los enlaces de salida. En este caso, aunque el arreglo es físicamente de estrella, lógicamente funciona como topología bus. La transmisión de una trama de cualquier estación es recibida por todas las estaciones y solo una estación puede transmitir a la vez. La otra forma de trabajo es cuando el nodo central funciona como equipo de swicheo de tramas. La trama que llega es almacenada en el nodo central y retransmitida únicamente sobre el enlace punto-punto existente entre la estación de destino y el nodo central.

4.1.2 Control de Acceso al Medio

Todas las LANs y WANs consisten en una colección de equipos que deben compartir la capacidad de transmisión de las redes y por tal motivo se debe compartir la capacidad de forma ordenada y eficiente, este es el trabajo del protocolo de control de acceso al medio (MAC). Los parámetros clave para cualquier técnica de control de acceso al medio son el dónde y cuándo. Dónde se refiere a si es requerido un control centralizado o distribuido. En un esquema centralizado, un controlador es designado con la autoridad para permitir acceso a la red. Si una estación desea transmitir debe esperar hasta recibir permiso del controlador. Si se está en una red descentralizada, las estaciones desempeñan colectivamente la función del controlador de acceso al medio para determinar dinámicamente el orden en el cual las estaciones transmitirán. El segundo parámetro (cuándo) está contenido en la topología y es un intercambio entre los factores de costo, desempeño y complejidad.

a) Formato de la Trama MAC Ethernet.

La capa MAC recibe un bloque de datos de la capa LLC y es la responsable de desempeñar funciones relacionadas con el acceso al medio y la transmisión de información. En general, todas las tramas MAC tienen un formato similar al que se muestra a continuación:

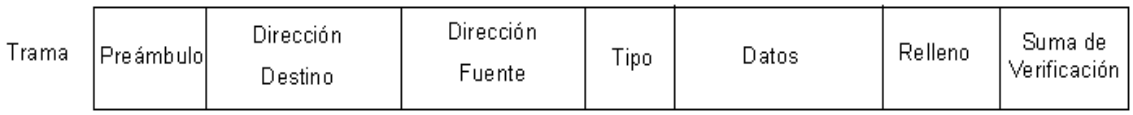


Figura 4.2 Formato de trama Ethernet

- Preámbulo: Este campo contiene el patrón de bits 10101010, que es utilizado para que el reloj del receptor se sincronice con el emisor.
- Dirección Destino: La dirección del destino físico en el LAN para la trama.
- Dirección Origen: La dirección de la fuente física en el LAN para la trama.
- Tipo: Indica al receptor qué hacer con la trama. Es posible utilizar múltiples protocolos de capa de red al mismo tiempo en la misma máquina, este campo indica qué proceso darle a la trama.

- Datos: es la información que se envía (hasta 1500 bytes).
- Relleno: es utilizado para completar 64 bytes. Para que Ethernet pueda diferenciar entre las tramas válidas y las tramas basura, se requiere que las tramas tengan una longitud mínima de 64 bytes. Si la porción de datos es menor que 46 bytes, este campo se utiliza para rellenar la trama al tamaño mínimo.
- Suma de Verificación: es una verificación de redundancia. Simplemente realiza la detección de errores, no la de corrección de errores.

b) Formato de la Trama MAC Inalámbrico

La capa MAC para las redes inalámbricas soporta 2 modos de funcionamiento, el primero llamado DCF (Función de Coordinación Distribuida) que no utiliza ningún tipo de control central y el segundo denominado PCF (Función de Coordinación Puntual).

El estándar 802.11 define tres clases diferentes de tramas en el cable: de datos, de control y de administración. Cada una de ellas tiene un encabezado con una variedad de campos utilizados dentro de la subcapa MAC. Además, hay algunos encabezados utilizados por la capa física.

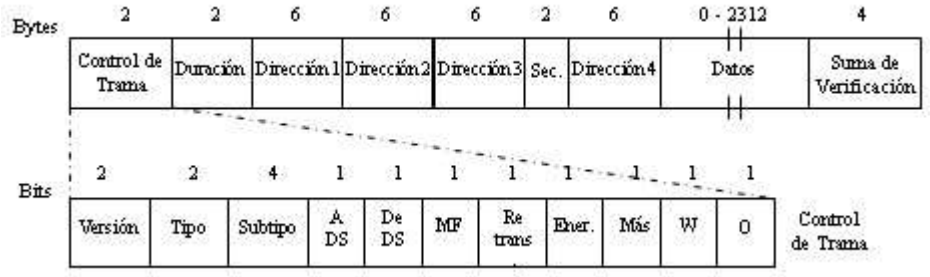


Figura 4.3 Formato de trama de datos 802.11

En la figura 4.3, se muestra el formato de la trama de datos. Empezaremos con el campo de Control de Trama, el cual tiene 11 subcampos:

- Versión de Protocolo: permite que dos versiones del protocolo funcionen al mismo tiempo en la celda.

- Tipo: Indica el tipo de trama, de datos, de control o administración.

- Subtipo: Indica el subtipo de la trama, por ejemplo: RTS o CTS.

- ADS y DeDS: Indica si la trama va o viene del sistema de distribución entre celdas.

- Bit MF: indica que siguen más fragmentos.

- Bit Retrans: marca una retransmisión de una trama que se envió anteriormente.

- Bit Administración de Energía: es utilizado por la estación base para poner al receptor en estado de hibernación o sacarlo de tal estado.

- Bit Más: indica que el emisor tiene tramas adicionales para el receptor.

- Bit W: especifica que el cuerpo de la trama se ha codificado utilizando el algoritmo WEP (Privacidad Inalámbrica Equivalente).

- Bit O: indica al receptor que una secuencia de tramas que tenga ese bit encendido debe procesarse en ese orden estricto.

Continuando con la trama original, tenemos como segundo campo a la DURACION, la cual indica cuánto tiempo ocuparán el canal la trama y su confirmación de recepción. Este campo también está presente en las tramas de control y es la forma mediante la cual las otras estaciones manejan el vector de asignación de red (NAV). El encabezado tiene cuatro DRECCIONES, una es para el origen y el destino, las otras 2 son utilizadas cuando las tramas entran o dejan una celda a través de una estación base especificándose la estación base de origen y destino para el tráfico entre celdas. El campo de SECUENCIA permite que se enumeren los fragmentos; de los 16 bits disponibles 12 identifican la trama y 4 el fragmento. El campo DATOS contiene la carga útil (hasta 2312 bytes). Por último tenemos el campo SUMA de VERIFICACIÓN.

Las tramas de administración tienen un formato similar al de las tramas de datos, excepto que no tienen una de las direcciones de la estación base, debido a que las tramas de administración se restringen a una sola celda. Las tramas de control son más cortas, tienen una o dos direcciones y no tienen campo de Datos, ni de Secuencia. La información clave en estas tramas se encuentra en el campo SUBTIPO, que por lo general son RTS, CTS o ACK.

4.2 Sistemas LAN

Ahora consideremos sistemas específicos LAN. Como sabemos, la técnica de control de acceso al medio y la topología son características clave utilizadas en la clasificación de las LAN en el desarrollo de estándares.

4.2.1 Ethernet y Fast Ethernet (IEEE 802.3)

La técnica más utilizada como control de acceso al medio para las topologías bus y estrella es el Acceso Múltiple con Detección de Portadora y Detección de Colisión (CSMA/CD)

a) Control de Acceso al Medio

Con el uso del acceso al múltiple con detección de portadora (CSMA), si una estación desea transmitir primero debe escuchar el medio para determinar si otra estación está transmitiendo, si el medio está en uso la estación debe esperar pero si está disponible puede empezar a transmitir. Puede ocurrir que dos o más estaciones intenten transmitir al mismo tiempo, si esto pasa ocurrirá una colisión y la información no será recibida exitosamente. La estación transmisora esperará una cierta cantidad de tiempo por una respuesta del receptor y si no llega se vuelve a retransmitir la información ya que se asume la presencia de una colisión. Para resolver este problema se utiliza una detección de colisión y se sigue el siguiente procedimiento:

1. Si el medio está disponible, se comienza la transmisión; de no estarlo se procede al paso 2.
2. Si el medio está ocupado, se continúa escuchando hasta que el canal esté libre, entonces se transmite.
3. Si una colisión es detectada durante la transmisión se envía una pequeña señal de bloqueo para comunicarle a todas las estaciones que hay una colisión y dejen de transmitir.
4. Después de transmitir la señal de bloqueo, se espera una cantidad de tiempo aleatoria y se vuelve a intentar la transmisión nuevamente.

b) Ethernet 10-Mbps

Hay definidas 5 alternativas de configuración física para una red de 10Mbps. Para identificarlos entre ellos se estableció la siguiente nomenclatura:

<Taza de Transferencia en Mbps> <Método de señalización> <Longitud máxima del segmento en cientos de metros>

Utilizando la nomenclatura anterior tenemos entonces las alternativas definidas por el comité IEEE 802.3 de la siguiente forma:

- 10BASE5
- 10BASE2
- 10BASE-T
- 10BASE-F

En donde T se refiere al par trenzado y F a fibra óptica.

i) Especificaciones del Medio 10Base5

Es la especificación original 802.3 del medio, que está basado directamente en Ethernet. Especifica el uso de cable coaxial de 50 ohms con señalización digital Manchester. La longitud máxima del segmento de cable es de 500 metros. La longitud de la red puede extenderse mediante el uso de repetidores, los cuales deben ser transparentes a nivel MAC. El estándar permite un máximo de 4 repetidores entre 2 estaciones limitando la longitud del medio a 2.5 kilómetros.

ii) Especificaciones del Medio 10Base2

Es de menor costo que el medio anterior. Utiliza cable coaxial de 50 ohms y señalización Manchester. La diferencia con el medio 10BASE5 es que el coaxial utilizado en más delgado. Debido a que manejan la misma taza de transferencia, es posible combinar segmentos 10BASE5 y 10BASE2. La única restricción existente es la de no colocar un segmento 10BASE2 para la unión de 2 segmentos 10BASE5, lo anterior es debido a que un segmento "backbone" debe ser tan resistente al ruido como los segmentos que conecta.

iii) Especificaciones del Medio 10Base-T

Sacrificando algo de distancia, es posible desarrollar una LAN de 10 Mbps utilizando cable par trenzado sin blindaje (UTP). Las especificaciones 10BASE-T definen a una topología estrella. Un sistema simple consiste en un número de estaciones conectadas a un punto central, definido como repetidor multipuerto, mediante 2 pares trenzados. La distancia de los segmentos se limita a 100 metros.

iv) Especificaciones del Medio 10Base-F

Las especificaciones de 10BASE-F permiten a los usuarios utilizar las ventajas de transmisión y distancia de la fibra óptica. El estándar contiene tres especificaciones:

- **10Base-FP (pasivo):** Es una topología estrella pasiva utilizada para interconectar estaciones y repetidores a distancias mayores a 1 km por segmento.
- **10Base-FL (enlace):** Define un en lace punto a punto que puede ser utilizado para conectar estaciones o repetidores a distancias superiores a 2 km.
- **10Base-FB (backbone):** Define un enlace punto a punto que puede ser utilizado para conectar repetidores a distancias superiores a 2 km.

Las tres especificaciones utilizan un par de fibras ópticas para cada enlace de transmisión, una para la transmisión en cada dirección. En cada caso la señalización utilizada es Manchester, la cual es posteriormente convertida a señal óptica.

c) IEEE 802.3 100-Mbps (Fast Ethernet)

Fast Ethernet son una serie de especificaciones desarrolladas por el comité IEEE 802.3 para proveer una LAN compatible con Ethernet operando a 100 Mbps de bajo costo. Se definieron un número de alternativas a utilizar con diferentes medios de transmisión. Todos los esquemas 100BASE-X utilizan dos enlaces físicos entre nodos, uno para la transmisión y otro para la recepción. 100BASE-TX utiliza cable par trenzado blindado (STP) o cable par trenzado sin blindaje categoría 5 (UTP). 100BASE-FX utiliza fibra óptica. Para todas las opciones 100BASE-T, la topología es similar a la 10BASE-T es decir una topología estrella.

i) Especificaciones 100BASE-X

Para todos los medios de transmisión especificados bajo 100BASE-X, una taza unidireccional de 100Mbps es alcanzada por la transmisión sobre un enlace sencillo (un solo par trenzado, una sola fibra óptica), por lo tanto para estos medios es requerido un esquema de codificación eficiente y efectivo. Para la transmisión 100BASE-X utilizamos la codificación 4B/5B-NRZI.

La designación 100BASE-X incluye dos especificaciones para medios físicos, uno para el par trenzado conocido como 100BASE-TX y el otro para la fibra óptica nombrado 100BASE-FX

ii) Especificaciones 100BASE-T4

Fue diseñado para producir una taza de transferencia de 100Mbps sobre un cable de categoría 3, aprovechando la ventaja de que ya se tenía instalado este tipo de cable en los edificios. Para 100BASE-T4 que utiliza cable categoría 3 para voz, no es razonable que alcance 100Mbps sobre un solo par trenzado y por tal motivo se especifica que la información debe ser dividida en 3 flujos de datos, cada uno con una taza de transferencia de 33 1/3Mbps. Se utilizan 4 pares trenzados, utilizando 3 pares para transmitir y recibir información. Dos de los pares deben estar configurados para la transmisión bidireccional.

4.2.2 LAN Inalámbrica

Se ha establecido un grupo de estándares para las redes inalámbricas, los cuales fueron desarrollados por el comité IEEE 802.11. Este estándar especifica tres técnicas de transmisión permitidas en la capa física, el método infrarrojo y los otros dos utilizan ondas de radio de corto alcance mediante técnicas como FHSS y DSSS. Las ondas de radio que se utilizan abarcan una parte del espectro radioeléctrico que no necesita licencia (banda ISM de 2.4GHz) que pueden funcionar a 1 o 2Mbps. En 1999 se introdujeron dos nuevas técnicas OFDM y HRDSSS, las cuales funcionan hasta 54Mbps y 11Mbps respectivamente.

a) IEE 802.11 LAN Inalámbrica de Baja Velocidad

Tomaremos 3 casos para LAN de baja velocidad. El primero corresponderá a la comunicación utilizando luz infrarroja, la cual utiliza transmisión difusa (no requiere línea visual) a 0.85 o 0.95 micras. Se permiten velocidades de 1 y 2Mbps. Las señales infrarrojas no pueden penetrar las paredes y por lo que las celdas en diferentes cuartos están bien aisladas. Sin embargo, debido al bajo ancho de banda es poco utilizada. En nuestro segundo caso tomaremos el método de modulación FHSS (Espectro Disperso con Salto de Frecuencia), el cual utiliza 79 canales en donde cada uno tiene un ancho de banda de 1MHz. En nuestro tercer caso tenemos la modulación DSSS (Espectro Disperso de Secuencia Directa), que tiene velocidades de 1 o 2Mbps.

b) IEEE 802.11a 54Mbps

Estas LAN utilizan OFDM (Multiplexión por División de Frecuencias Ortogonales) para enviar hasta 54Mbps en la banda ISM más ancha de 5GHz. Se utilizan 52 frecuencias diferentes 48 para datos y 4 para sincronización. Debido a que las transmisiones están presentes en múltiples frecuencias al mismo tiempo, esta técnica se considera como forma de espectro disperso.

c) IEEE 802.11b 11Mbps

Es otra técnica de espectro disperso llamada HR-DSSS (Espectro Disperso de Secuencia Directa de Alta Velocidad), que utiliza 11 millones de chips por segundo para alcanzar 11Mbps en la banda de 2.4GHz. Es importante hacer notar que este estándar no es continuación del 802.11a. Este estándar soporta tasas de datos de 1, 2, 5.5 y 11Mbps.

4.3 Dispositivos LAN

¿Por qué no usar una LAN mayor en lugar de 2 redes separadas? Existen varias razones por las cuales se utilizan los puentes para unir 2 redes LAN:

Confiabilidad: el riesgo de tener conectados todos los equipos de procesamiento de datos a una sola red es tal que si fallara la red, todos los equipo estarían incomunicados. Utilizando puentes, la red puede estar fragmentada en unidades autosuficientes.

Desempeño: en general, el desempeño de una LAN decae con el incremento de equipos que se conectan o por la longitud del cable. Un número de pequeñas redes puede ofrecer un aumento en el desempeño de la misma.

Seguridad: el establecer múltiples redes puede incrementar la seguridad en la comunicación. Es deseable mantener diferentes tipos de tráfico que tienen diferentes necesidades de seguridad en medios físicos separados. Al mismo tiempo, los diferentes tipos de usuarios con diferentes niveles de seguridad requieren comunicarse a través de mecanismos controlados y monitoreados.

Geografía: dos redes separadas se requieren para soportar equipos agrupados en 2 sitios geográficamente distantes. Si en el caso de que 2 edificios estén separados por una carretera, es mucho más fácil el uso de un puente por microondas en lugar de utilizar un enlace de cable coaxial entre los 2 edificios.

A los dispositivos que se conectan directamente a un segmento de red se les suele llamar host. Estos incluyen computadoras, impresoras, escáneres y muchos otros dispositivos. Los dispositivos host pueden existir sin una red, pero sus posibilidades serían muy limitadas. La función básica de las computadoras de la LAN es suministrar al usuario el mayor número de prestaciones posibles.

4.3.1 Tarjetas de interfaz de red

Estos dispositivos disponen de una conexión física con los medios de red a través de una tarjeta interfaz de red (NIC), la cual posee un código único en todo el mundo denominado dirección de control de acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host dentro de una red. La NIC es el componente de hardware más básico en las comunicaciones de red. Traduce la señal paralela producida por la computadora en un formato serie que se envía mediante el cable de red. La comunicación binaria (unos y ceros) se transforma en impulsos eléctricos, pulsos de luz, ondas de radio o cualquier esquema de señal que usen los medios de red.

En algunos casos, el conector de la NIC no coincide con el tipo de medio al que necesita conectarse y para lograr la conexión se emplea un transceptor (transmisor/receptor). Un transceptor convierte un tipo de señal y / o conector en otro. Un ejemplo de un transceptor es la conversión de señales eléctricas (UTP) a señales ópticas (Fibra Óptica).

a) **b)**

Figura 4.4 Tarjeta de interfaz de red. a) Tarjeta WLAN. b) Tarjeta LAN

4.3.2 Repetidores

Existen muchos tipos de medios y cada uno tiene sus ventajas y desventajas. Una de las desventajas del tipo de cable UTP categoría 5 es su longitud máxima, la cual debe ser de aproximadamente 100m. Si se necesita extender la red más allá de este límite, se debe añadir un dispositivo de red denominado repetidor. Para comenzar a entender el funcionamiento de este dispositivo, es importante comprender que un dato abandona el origen y se mueve por la red, transformándose en pulsos de luz o eléctricos que pasan por los medios de red. Estos pulsos se llaman señales. Cuando las señales abandonan un puesto de transmisión, están limpias y son fácilmente reconocibles, pero la longitud del cable deteriora y debilita las señales mientras pasan por los medios de red. Por ejemplo como ya se mencionó, la longitud máxima del cable UTP categoría 5 es de 100m, si se excede tal distancia no hay garantía de que una tarjeta de red pueda leer la señal. Un repetidor puede solucionar este problema.

El propósito del repetidor es regenerar y reenviar las señales de red al nivel de bits para hacer posible que estas viajen largas distancias por los medios de transmisión. Hay que tener mucho cuidado con la regla 5-4-3 cuando utilizamos Ethernet 10Mbps, en donde se dice que se pueden conectar cinco segmentos de red de extremo a extremo utilizando cuatro repetidores, pero solo tres segmentos podrán tener hosts. El repetidor es un dispositivo de la capa física en el modelo de referencia OSI.

4.3.3 Hubs

En general, el término hub se emplea en lugar de repetidor cuando se refiere al dispositivo que es utilizado como centro de la red o nodo central. Aunque un hub opera en una topología física estrella, crea el mismo entorno de contención que una topología bus. Esto se debe a que cuando un dispositivo transmite, el resto de los dispositivos escuchan y la contención crea un bus lógico.

El propósito de un hub es regenerar y reenviar señales de red. Esto se hace a nivel de bit con un gran número de host (4, 8 o 24). Esta acción se conoce como concentración. Las propiedades más importantes de los hubs son:

- Regenerar y reenviar las señales.
- Propagar las señales.
- No pueden filtrar tráfico de la red.
- No pueden determinar la mejor ruta.
- Se utilizan como puntos de concentración de la red.

Ya habrá notado que las características de un hub son similares a las de los repetidores, y se debe a que los hubs también se les conoce como repetidores multipuerto. La diferencia radica en el número de cables que se conectan al dispositivo. Mientras que un repetidor normalmente solo tiene dos puertos, un hub generalmente tiene cuatro o más puertos. El repetidor recibe en un puerto y repite en el otro, en un hub se recibe en un puerto y se repite en el resto. El hub es un dispositivo que al igual que los repetidores trabaja en la capa 1 del modelo de referencia OSI.

4.3.4 Puentes

Un puente es un dispositivo diseñado para crear dos o más segmentos LAN, cada uno de ellos con un dominio de colisión separado. En otras palabras, han sido creados para crear un ancho de banda más utilizable. El propósito de un puente es filtrar el tráfico de las LAN, para mantener el tráfico local, permitiendo la conectividad con otras partes de la LAN para el tráfico que se dirige allí. La diferencia entre el tráfico local y el que no lo es se logra gracias a la dirección MAC. El puente controla qué direcciones MAC tiene en cada lado y toma sus decisiones basándose en las direcciones MAC.

Los puentes filtran el tráfico de red revisando solo las direcciones MAC y por tanto, pueden enviar rápidamente tráfico representando cualquier protocolo da capa de red. Los puentes se preocupan solo de las tramas que pasan, basándose en las direcciones MAC de destino. Las siguientes son las propiedades más importantes de los puentes:

- Son más inteligentes que los hubs, ya que pueden analizar las tramas que llegan y enviarlas basándose en la información de dirección.
- Recogen y pasan paquetes entre dos o más segmentos LAN.
- Crean más dominios de colisión, permitiendo que más de un dispositivo pueda retransmitir simultáneamente sin provocar una colisión.
- Mantienen las tablas de dirección MAC.

4.3.5 Switches

Un switch, en ocasiones se le denomina puente multipuerto, al igual que al hub se le llama repetidor multipuerto. La diferencia entre un hub y el switch es la misma que ente un repetidor y un puente: los switches toman decisiones basándose en las direcciones MAC y los hubs, sencillamente no toman decisiones.

Gracias a las decisiones tomadas por los switches, las LAN son mucho más eficientes. Lo consiguen conmutando los datos fuera del puerto al que el propio host está conectado. Por su parte, un hub envía datos a todos los puertos para que todos los hosts tengan que ver y procesar (aceptar o rechazar) todos los datos. Los switches se parecen a

los hubs físicamente, ya que ambos tienen muchos puertos de conexión, porque parte de su función es la concentración de la conectividad (permitir que muchos dispositivos estén conectados a un punto de la red) pero la diferencia radica en lo que sucede en el interior del dispositivo, el propósito de un switch es conmutar las tramas de los puertos entrantes a los puertos salientes mientras proporciona a cada puerto un ancho de banda completo.

4.3.6 Ruteadores

El ruteador es un dispositivo que toma decisiones basándose en las direcciones de red (Capa 3 modelo OSI), al contrario de las direcciones MAC individuales (Capa 2 modelos OSI). Los ruteadores pueden conectar diferentes tecnologías como Ethernet, Token Ring y FDDI. Debido a su capacidad de enrutar paquetes en base a la información de red, estos equipos se han convertido en el backbone de Internet, ejecutando el protocolo IP.

El propósito de un ruteador es examinar los paquetes entrantes, elegir la mejor ruta y conmutarlos al mejor puerto de salida. Los ruteadores son el dispositivo regulador de tráfico más importante en las redes, debido a que permiten que cualquier tipo de computadora se comunique con otra en cualquier parte del mundo. Los ruteadores difieren de los puentes en dos aspectos importantes, el primero es que los ruteadores trabajan en la capa 3 y los puentes en la capa 2; el segundo aspecto es que los puentes utilizan direcciones MAC para tomar decisiones, mientras que los ruteadores utilizan un esquema de direcciones diferente para tomar las decisiones de envío. Los ruteadores utilizan direcciones llamadas Protocolo IP (IP), o direcciones lógicas. Los ruteadores equiparan la información de la tabla de enrutamiento con las direcciones IP de destino de los datos y envían los datos entrantes hacia la subred y el host correctos. Como las direcciones IP se implementan en el software y hacen referencia a la red en la que está ubicado el dispositivo, a veces estas direcciones son llamadas direcciones de protocolo o direcciones de red.

CAPITULO 5

ARQUITECTURA DE COMUNICACIONES Y PROTOCOLO

Los conceptos de procesamiento distribuido y la interconexión de computadoras implican que entidades de diferentes sistemas se comuniquen. Algunos ejemplos de estas entidades son aplicaciones de programas, transferencia de archivos, sistemas de manejo de bases de datos, correo electrónico y terminales. Ejemplos de sistemas son las computadoras, terminales y censores remotos. En general una entidad es todo aquello capaz de enviar o recibir información y un sistema es un objeto físico que contiene una o más entidades. Para que dos entidades se comuniquen exitosamente, deben hablar el mismo idioma. ¿Qué es comunicado?, ¿cómo es comunicado?, ¿cuándo es comunicado? conforman un grupo de convenios que involucrados en la comunicación son llamados protocolos.

5.1 Protocolo y Arquitectura

Un protocolo es una serie de reglas de comunicación entre dispositivos similares. Pueden cubrir cualquier cosa, pero en general los protocolos regulan condiciones como a quien le toca transmitir, como son detectados y arreglados los errores, así como la distinción entre datos y señales enviadas entre ellos.

Los elementos clave de un protocolo son:

- Sintaxis: el formato de la información, codificación y niveles de señal.
- Semántica: información de control para coordinar y manejar los errores.
- Tiempo: la velocidad de secuencia y emparejamiento.

Los protocolos fueron diseñados originalmente por compañías como IBM y Novell ocasionando la dificultad en la comunicación entre equipos de diversas marcas. Para resolver este problema la Organización de Estándares Internacional (ISO) desarrolló un estándar llamado OSI (Interconexión de Sistemas Abiertos), quien define 7 capas diferentes de protocolos. Cada capa es responsable de una función diferente e independiente de las otras capas. Los protocolos no siguen el modelo OSI exactamente, pero los profesionales frecuentemente se refieren a ellos, por tal motivo es importante conocerlos. La arquitectura del modelo OSI se compone de 7 capas:

1. Capa Física: se ocupa de la transmisión del flujo de bits sobre el medio físico; maneja las características mecánicas, eléctricas, funcionales y procedimientos para acceder al medio físico.
2. Capa de Enlace de Datos: envía los bloques de información (tramas) con la sincronización necesaria, control de error y control de flujo.
3. Capa de Red: provee independencia a las capas superiores de la transmisión de información y tecnología de conmutación utilizada para conectar los sistemas; es responsable de establecer, mantener y terminar las conexiones.
4. Capa de Transporte: provee transferencia de información entre extremos; provee control de flujo y recuperación de error entre ambos extremos.
5. Capa de Sesión: provee la estructura de control para la comunicación entre aplicaciones; establece, controla y termina las conexiones (sesiones) entre aplicaciones.
6. Capa de Presentación: provee independencia al proceso de aplicación de diferencias en la presentación de la información (sintaxis).

7. Capa de Aplicación: provee acceso al ambiente OSI para los usuarios así como servicios de información distribuida.

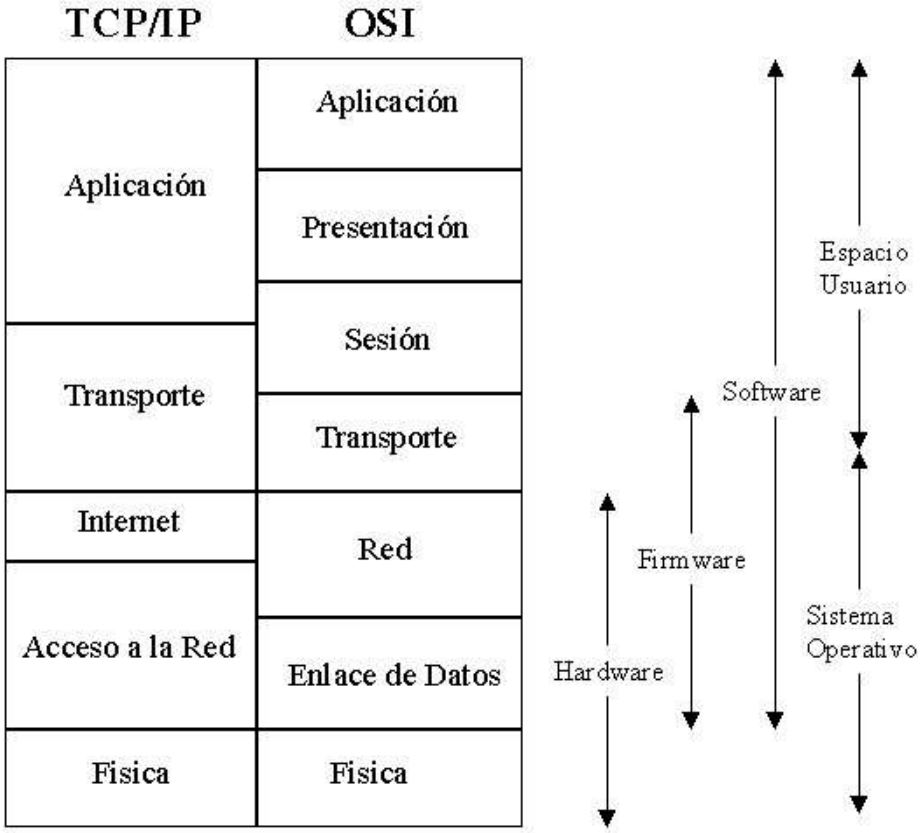


Figura 5.1 Comparación entre Modelos OSI y TCP/IP

El protocolo TCP/IP es más comúnmente utilizado y OSI ha sido un modelo estándar para la clasificación de las funciones de comunicación. TCP/IP es el resultado de una investigación de protocolos desarrollados para las redes experimentales de conmutación de paquetes. Consiste en una colección de protocolos que han sido publicados como estándares de Internet. No hay modelo oficial como lo hay en el caso de OSI, pero basados en los protocolos estándares se pueden organizar de la siguiente forma:

1. Capa Física: cubre la interfase física entre el equipo de transmisión de información (computadora) y el medio de transmisión o red.
2. Capa de Acceso a la Red: se ocupa del intercambio de información entre un sistema y la red a la cual está unida.

3. Capa de Internet: se utiliza el protocolo de Internet (IP) para proveer la función de ruteo a través de múltiples redes, cuando se desean comunicar equipos de diferentes redes.
4. Capa de Transporte: el protocolo de control de transmisión (TCP) es utilizado para asegurar que toda la información enviada llegue al destino.
5. Capa de Aplicación: contiene la lógica requerida para soportar varias aplicaciones.

5.2 Interconexiones

Un grupo de redes interconectadas desde el punto de vista del usuario, se apreciaría como una gran red. Sin embargo, si cada una de las redes conserva su identidad se requieren de mecanismos especiales para la comunicación entre múltiples redes englobando todas las redes como Internet y a cada red que la constituye se le denomina subred. Cada subred debe soportar la comunicación entre los equipos que conforman esa subred, denominados sistemas terminales (ES) y la Internet. Las subredes están conectadas a la Internet por equipos denominados sistemas intermedios (IS) que pueden ser puentes o ruteadores. La diferencia entre un puente y un ruteador radica en que el primero trabaja sobre la capa 2 del modelo OSI para conectar redes iguales y el segundo sobre la capa 3 del mismo modelo y puede conectar redes diferentes.

Los principios de las interconexiones de redes se pueden resumir en los siguientes puntos:

- Proveer un enlace entre redes como mínimo requiere una conexión física y control de enlace.
- Proveer el ruteo y entrega de información entre procesos de diferentes redes.
- Proveer una cuenta de servicio que mantenga rutas de uso de varias redes y ruteadores así como mantener un estatus de información.
- Proveer los servicios enlistados anteriormente de forma tal que no se requiera modificación de la arquitectura de red de las subredes.

5.2.1 Protocolo de Internet

Este protocolo es parte del conjunto de protocolos TCP/IP y es el más utilizado para la interconexión entre redes. Como cualquier otro protocolo estándar, IP se especifica en dos partes, primero es por la interfaz con la capa superior especificando los servicios que proporciona y segundo, es el formato real del protocolo con sus mecanismos asociados. El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP mostrado en la figura 5.2. Los campos son los siguientes:

- Versión (4 bits): indica el número de la versión del protocolo.
- Longitud de la cabecera de Internet (IHL) (4 bits): es la longitud de la cabecera expresada en palabras de 32 bits.
- Tipo de Servicio (8 bits): especifica los parámetros de seguridad, prioridad, retardo y rendimiento.
- Longitud Total (16 bits): longitud total del datagrama en octetos.
- Identificador (16 bits): número de secuencia que en conjunto con la dirección de origen, destino y el protocolo se utilizan para identificar al datagrama.
- Indicadores (3 bits): Se han definido 2 de los tres bits. El bit “Mas” es utilizado para segmentar y reensamblado. El bit “No Fragmentación” prohíbe la fragmentación cuando tiene el valor 1.
- Desplazamiento del Fragmento (13 bits): indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits.
- Tiempo de Vida (8 bits): medido en saltos de dispositivos de ruteo.
- Suma de comprobación de cabecera (16 bits): solamente se aplica a la cabecera un código de detección de errores. Ya que algunos campos de la cabecera pueden cambiar durante el viaje, este valor se verifica y recalcula en cada ruteador.
- Dirección Origen (32 bits): codificada para permitir una asignación variable de bits para especificar la red y el sistema final conectado a la red especificada.
- Dirección Destino (32 bits): igual que la dirección de origen.

- Opciones (variable): contiene las opciones solicitadas por el usuario que envía los datos.
- Relleno (variable): se usa para asegurar que la cabecera del datagrama tenga una longitud múltiplo de 32 bits.
- Datos (variable): el campo de datos debe tener una longitud múltiplo de 8bits. La máxima longitud de un datagrama es de 65535 octetos, incluyendo campo de datos y cabecera.

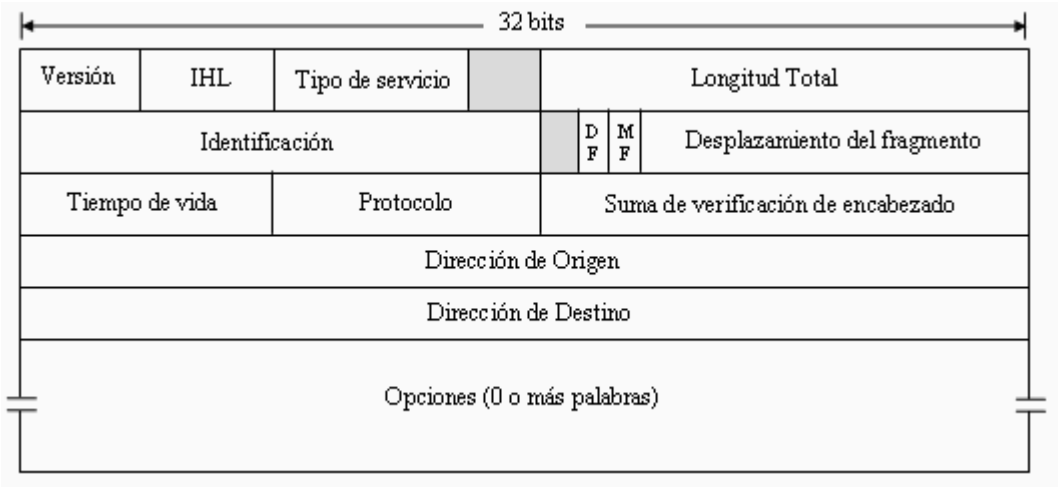


Figura 5.2 Referencia encabezado IP

Los campos de origen y destino en la cabecera IP contienen cada uno una dirección Internet global de 32 bits, que generalmente consiste de un identificador de red y un identificador del equipo (host). La dirección es única, no debe haber 2 equipos con la misma dirección IP. Las direcciones IP se dividen en clases, las cuales están ilustradas en la figura 5.3

Figura 5.3 Clases de redes

5.3 Protocolo de Transporte

El protocolo de transporte es el corazón de toda la jerarquía de protocolos. La meta fundamental de la capa de transporte es proporcionar un servicio eficiente, confiable y económico a sus usuarios. Existen 2 tipos de servicio de transporte, el orientado a la conexión que es similar a la conmutación de paquetes por circuitos virtuales y el no orientado a la conexión que es muy similar a la conmutación de paquetes por datagramas.

Hay dos protocolos principales para la capa de transporte, uno orientado a la conexión que se llama TCP (Protocolo de Control de Transporte) y el segundo que es no orientado a la conexión denominado UDP (Protocolo de Datagrama de Usuario). Ambos protocolo se explicarán brevemente.

5.3.1 Protocolo de Datagrama de Usuario (UDP)

Este protocolo transmite segmentos que consisten en un encabezado de 8 bytes seguido de la carga útil. Los puertos sirven para identificar los puntos terminales dentro de las máquinas de origen y destino, esto es que cuando llega un paquete UDP, la carga útil se entrega al proceso que está enlazado al puerto destino. Sin los campos de puerto, la capa de transporte no sabría que hacer con el paquete.

Figura 5.4 Encabezado UDP

De la figura 5.4 se puede apreciar el encabezado que utiliza UDP en donde además de los puertos de origen y destino, hay un campo denominado longitud UDP, el cual incluye el encabezado de 8 bytes así como los datos. El campo suma de verificación UDP es opcional. El protocolo UDP no realiza control de flujo, control de errores o retransmisión cuando se recibe un segmento erróneo.

5.3.2 Protocolo de Control de Transporte (TCP)

El protocolo TCP se diseñó específicamente para proporcionar un flujo de bytes confiables de extremo a extremo sin importar topologías, anchos de banda, retardos y otros parámetros que se pueden presentar cuando se viaja por diversas redes. Toda máquina que soporta TCP cuenta con una entidad de transporte TCP, la cual puede ser un procedimiento de biblioteca o un proceso de usuario. Una entidad TCP acepta flujos de datos de usuario de procesos locales, los divide en fragmentos que no sobrepasen los 64Kb y envía cada fragmento como un datagrama IP independiente. Al llegar los datagramas al destino, la entidad TCP reconstruye los flujos de bytes originales. Debido a que la capa IP no proporciona garantía de que los datagramas se entregarán de manera apropiada o pueden llegar en el orden incorrecto, corresponde a TCP resolver estos detalles. Todas las conexiones TCP son full duplex.

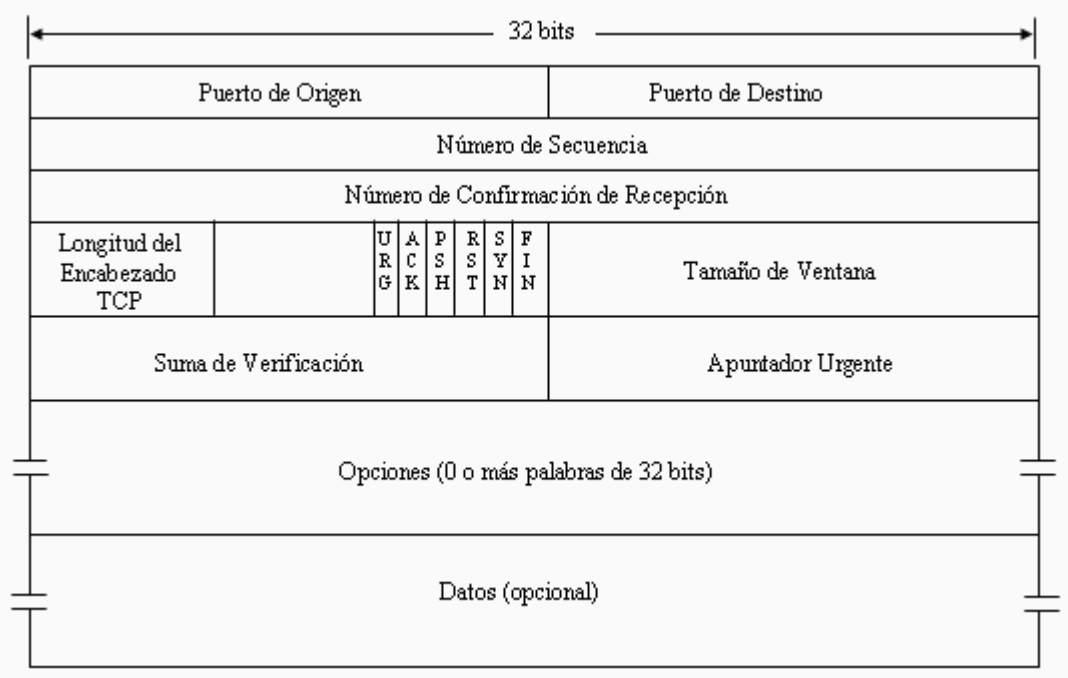


Figura 5.5 Encabezado TCP

El servicio TCP se obtiene al hacer que tanto el servidor como el cliente creen puntos terminales denominados sockets. Cada socket tiene un número (dirección), el cual consiste en la dirección IP del equipo (host) y un número de 16 bits que es local a ese

equipo (host) llamado puerto. Para obtener un servicio TCP, se debe establecer una conexión entre un socket en la máquina emisora y uno en la máquina receptora. Ahora se explicará el encabezado TCP tal como se explicó en el protocolo UDP.

En la figura 5.5 se pueden apreciar los campos que conforman el segmento TCP. Cada segmento comienza con un encabezado de formato fijo de 20bytes. Comencemos con la separación del encabezado TCP campo por campo.

- Puerto de origen: identifica el punto terminal local de la conexión en la fuente.
- Puerto de destino: identifica el punto terminal local de la conexión en el destino.
- Número de Secuencia: hace referencia al primer octeto en campo de datos.
- Número de Confirmación de Recepción: especifica el siguiente byte esperado.
- Longitud del Encabezado TCP: indica la cantidad de palabras de 32bits contenidas en el encabezado TCP. Es importante ya que el campo opciones es de longitud variable.
- URG: si este apuntador tiene el valor de 1 se especifica se indica que el apuntador urgente está en uso.
- ACK: utilizado para indicar que el número de confirmación de recepción es válido.
- PSH: indica que los datos se deben de transmitir de inmediato. Se solicita al receptor que entregue los datos a la llegada y no los almacene en memoria.
- RST: se utiliza para reestablecer una conexión, rechazar un segmento no válido o un intento de abrir una conexión.
- SYN: se utiliza para establecer una conexión.
- FIN: es utilizado para liberar una conexión.
- Tamaño de Ventana: indica la cantidad de bytes que pueden enviarse comenzando por el byte cuya recepción se ha confirmado, ya que se utilaza como control de flujo el método de ventana corrediza.
- Suma de verificación: se utiliza para agregar confiabilidad.

- Opciones: ofrece una forma de agregar características extra no cubiertas por el encabezado normal.

5.3.3 TCP y UDP Inalámbricos

En teoría, los protocolos de transporte deben ser independientes de la tecnología de la capa de red subyacente. En particular, TCP no debería preocuparse si el IP está operando por fibra o por radio. En la práctica si importa, puesto que la mayoría de las implementaciones del TCP han sido optimizadas con base en supuestos de las redes alámbricas, pero no en las inalámbricas. Ignorar las propiedades de la transmisión inalámbrica puede conducir a implementaciones TCP correctas lógicamente pero de un desempeño horrendo. El problema principal es el control de congestionamiento, ya que las expiraciones del temporizador ocurren por congestionamientos, no por paquetes perdidos. En consecuencia, al expirar el temporizador, el TCP disminuye su velocidad.

Desafortunadamente, los enlaces inalámbricos son poco confiables dado que pierden paquetes todo el tiempo. El enfoque adecuado par el manejo de paquetes perdidos es enviarlos nuevamente tan pronto como sea posible. La reducción de la velocidad simplemente empeora las cosas. Supongamos que se pierde un 20% de todos los paquetes, entonces cuando un emisor envía 100 paquetes/seg, la velocidad real de transporte es de 80 paquetes/seg.

Si bien el UDP no tiene los mismos problemas que TCP, la comunicación inalámbrica también le produce dificultades. El problema es que los programas utilizan el UDP pensando que es altamente confiable y en un entorno inalámbrico, UDP está muy lejos de serlo. En aquellos programas capaces de recuperarse de la pérdida de mensajes UDP, pasar de un entorno en el que rara vez se pierden mensajes, a uno en el que constantemente se pierden, puede dar pie a un desempeño desastroso.

5.4 Seguridad en Redes

La meta de la seguridad en una red es permitir que usuarios autorizados puedan acceder a la información y servicios de la red en tanto que los usuarios no autorizados no

puedan entrar a la red. Muy comúnmente al incrementar la seguridad de la red, la eficiencia de la misma disminuye. Los canales por los cuales se transmiten los datos son inherentemente inseguros, por tal motivo toda información privada que se transmite por estos canales debe ser protegida.

Para asegurar la información se puede encriptar su contenido. La criptografía que viene del griego y significa "escritura secreta" transforma la información mediante un encriptador o criptosistema (algoritmo matemático para encriptar mensajes). Muchos hacen una diferenciación entre cifrados y códigos, un cifrado es una transformación carácter por carácter o bien bit por bit, sin importar la escritura lingüística del mensaje. Un código reemplaza una palabra con otra palabra o símbolo. La llave que es una cadena de dígitos que actúa como contraseña, es integrada por el encriptador, quien utiliza la llave para transformar la información a una forma incomprensible para todos exceptuando al que envía la información y el receptor al que se desea enviar dicha información.

La información que no está encriptada se le denomina "Texto Llano" y a la información que contiene encriptación es conocida como "Texto Cifrado". El algoritmo es el responsable para la encriptación de los datos, mientras que la llave actúa como una variable. El uso de diferentes llaves origina diferentes textos cifrados. Solamente el destinatario al que se desea enviar la información debe tener la llave correspondiente para descifrar el texto cifrado en texto llano. El arte de descifrar los mensajes (criptoanálisis) y el arte de crear los cifrados (criptografía) se conoce en conjunto como criptología. La idea de que el criptoanalista conozca los algoritmos y que la naturaleza secreta se base principalmente en las claves se conoce como principio de Kerckhoff, que debe su nombre al critógrafo militar holandés Auguste Kerckhoff, establecido en 1883:

Principio: *Todos los algoritmos deben ser públicos, solo las claves deben ser secretas*.

Tratar de mantener secreto el algoritmo, se le conoce como seguridad por desconocimiento, nunca funciona.

5.4.1 Algoritmos de Encriptación

La criptografía moderna utiliza las mismas ideas básicas que la criptografía tradicional (la transposición y la sustitución), pero la orientación es distinta. Tradicionalmente los criptógrafos han usado algoritmos; hoy en día se hace lo opuesto: el objetivo es hacer algoritmos de encriptación tan complicados que incluso si el criptoanalista obtiene cantidades enormes de texto cifrado, no será capaz de entender nada sin la clave. Los algoritmos criptográficos pueden implementarse en hardware (para velocidad) y en software (para flexibilidad).

a) Algoritmo de Clave Secreta

En el pasado, las organizaciones deseban mantener un ambiente computacional seguro utilizando criptografia simétrica, conocida también como criptografía de clave secreta. Esta criptografía utiliza la misma clave para encriptar y desencriptar. En este caso, el remitente encripta un mensaje utilizando la clave secreta y después envía el mensaje a su destino. El problema con este algoritmo es que se debe encontrar un camino seguro para intercambiar la llave secreta antes de establecer la comunicación de forma segura. Una opción sería el uso de un mensajero. Aunque este método de envío de calve es factible cuando se comunican dos personas, no es eficiente para asegurar la seguridad de la comunicación en una red grande. La privacidad y la integridad del mensaje estarían comprometidas si la clave secreta es interceptada. También, si ambas partes en una transacción utilizan la misma clave para encriptar y desencriptar, uno no podría autentificar cual de las partes ha creado el mensaje. Finalmente, para mantener la comunicación privada con cada receptor, un remitente requiere de diferentes claves, una para cada receptor.

Uno de los algoritmos con encriptación simétrica que más se utiliza es el “Estándar de Encriptación de Datos” (DES), el cual utiliza una llave con longitud de 56 bits para encriptar información en bloques de 64 bits. Este tipo de encriptación es conocido también como cifrado de bloques. El cifrado de bloques es un método de encriptación

que crea grupo de bits de un mensaje original, después aplica un algoritmo de encriptación al bloque en lugar de aplicarlo a cada bit individualmente. Este método reduce la cantidad de procesos y tiempo requerido, manteniendo un nivel de seguridad confiable. Sin embargo DES se considera inseguro. A finales de los 90 se reemplazó el DES por el triple DES (3DES). En esencia, la variante consiste en un arreglo de tres sistemas DES en fila, cada uno con su propia calve secreta. El 3DES es más seguro pero más lento. Otro estándar es el "Estándar de Encriptación Avanzada" (AES) que utiliza el método de encriptación Rijndael, el cual puede ser utilizado con calves y bloques de 128, 192 y 256 bits. El método Rijndael fue elegido por su alta seguridad, desempeño, eficiencia, flexibilidad y poco requerimiento de memoria para los sistemas de cómputo.

b) Algoritmo de Clave Pública

El problema de distribución de claves ha sido la parte débil de la mayoría de los criptosistemas. Sin importar lo robusto del sistema, si un intruso roba la clave, el sistema no vale nada. Siempre se había tomado que las claves de encriptación y desencriptación eran las mismas o la clave para desencriptar se podía derivar de la clave de encriptación. Las claves tenían que distribuirse a todos los usuarios y por tanto había un problema: las claves deben protegerse contra robo, pero deben estar disponibles para los usuarios.

En 1976, los investigadores Diffie y Hellman de la Universidad de Stanford propusieron un nuevo criptosistema en donde las claves de encriptación y desencriptación eran diferentes, también la clave para desencriptar no se podía derivar de la clave de encriptación. En la propuesta, el algoritmo de encriptación (E) y el algoritmo de desencriptación (D) tenían que cumplir los siguientes requisitos:

1.- $D(E(P)) = P$

2.- Es excesivamente difícil deducir D de E.

3.- E no puede descifrarse mediante un ataque de texto llano seleccionado.

El primer punto se refiere a que si aplicamos D a un mensaje cifrado E(P), obtenemos nuevamente el mensaje de texto llano original P.

El método funciona de la siguiente forma. Una persona, llamémosla Alicia, que desea recibir mensajes secretos, primero diseña dos algoritmos E_A y D_A que cumplan los requisitos anteriores. El algoritmo de encriptación y la clave de Alicia se hacen públicos, en este caso la puede tener en su página de Internet. Utilizaremos la notación E_A para denotar el algoritmo de encriptación parametrizado por la clave pública de Alicia. De igual forma, el algoritmo de desencriptación (secreto) parametrizado por la clave privada de Alicia es D_A. Benito hace lo mismo, haciendo pública E_B pero manteniendo secreta D_B.

Ahora veremos si podemos resolver el problema de establecer un canal seguro entre Alicia y Benito, que nunca han tenido contacto previo. Se supone que las claves de encriptación E_A y E_B, están en un archivo de lectura pública. Alicia toma su primer mensaje P, calcula $E_B(P)$ y lo envía a Benito. En el otro extremo Benito desencripta el mensaje aplicando su clave secreta D_B [es decir, calcula $D_B(E_B(P)) = P$]. Para que Benito pueda emitir una respuesta (R), transmite $E_A(R)$. Ahora Alicia y Benito se pueden comunicar con seguridad.

5.4.2 Protocolos de Seguridad

Se discutirán los protocolos de seguridad para las redes como lo son el Protocolo de Seguridad de Internet (IPSec) y el protocolo de seguridad de la capa de transporte como la Capa de Socket Seguro (SSL). Los protocolos de seguridad protegen las comunicaciones entre las redes; los protocolos de seguridad de la capa de transporte son para establecer una conexión segura por la cual pueda transitar la información.

a) Capa de Socket Seguros (SSL)

Actualmente la mayoría del comercio electrónico (e-business) utiliza SSL para la seguridad de las transacciones en línea, aunque SSL no fue diseñado para asegurar transacciones. El protocolo SSL fue desarrollado por Netscape Communications, es un protocolo sin propietario utilizado comúnmente para asegurar la comunicación entre dos computadoras en Internet. SSL está incluido en los exploradores de Internet así como en

numerosos productos de software. Este protocolo opera entre el protocolo de comunicación de Internet TCP/IP y el software de aplicación.

En una comunicación sobre Internet, el remitente envía un mensaje, el cual pasa por un "socket", quien recibe y transmite información de una red. El socket entonces interpreta el mensaje mediante el Protocolo TCP/IP. El Protocolo TCP/IP es el set de protocolos estándar utilizado para la conexión de computadoras y redes con la Internet. La mayaría de las transmisiones en Internet son enviadas como conjuntos de piezas individuales del mensaje, denominados paquetes. En el extremo del remitente, los paquetes de un mensaje son enumerados en forma secuencial, además se incluye al paquete información sobre el control de errores. IP es responsable del ruteo de paquetes con el fin de evitar congestionamientos, de esta forma cada paquete puede viajar por una ruta diferente sobre Internet. El destino de los paquetes es determinado por la dirección IP. En el extremo del destinatario, TCP se asegura que todos los paquetes lleguen, los acomoda en orden secuencial y determina si los paquetes han arribado con alteraciones. En caso de tener paquetes alterados o algunos datos han sido pedidos, TCP solicita la retransmisión. Sin embargo, TCP no determina si un paquete ha sido intencionalmente alterado durante la transmisión y los paquetes alterados pueden se tomados como válidos. Una vez que todos los paquetes llegan, el mensaje es enviado al socket del destinatario quien traduce el mensaje a un formato que puede ser recibido por la aplicación. En una transacción que se utilice SSL, los sockets son asegurados utilizando criptografía de clave pública.

SSL implementa la tecnología de calve pública utilizando el algoritmo RSA y un certificado de autenticidad para validar el servidor en una transacción y así proteger la información privada enviada de un extremo a otro sobre la Internet.

Aún y cuando el protocolo SSL protege la información cuando ésta atraviesa la Internet, no puede proteger información confidencial como lo es el número de tarjetas de crédito cuando ésta es almacenada en el servidor del destinatario. Cuando un destinatario

recibe información confidencial como este caso y no es encriptada para su almacenamiento, es probable que una persona pueda acceder a dicha información.

b) Protocolo de Seguridad de Internet (IPSec)

Las redes permiten a una organización la conexión de múltiples equipos. Actualmente las organizaciones utilizan la infraestructura existente de Internet para crear Redes Privadas Virtuales (VPN), uniendo múltiples redes, usuarios inalámbricos y usuarios remotos. La encriptación permite a la VPN proveer los mismos servicios de una red privada sobre una red pública.

Una VPN es creada estableciendo un túnel seguro por el cual los datos atraviesan múltiples redes sobre Internet. IPSec (Protocolo de Seguridad de Internet) es una de las tecnologías utilizadas para asegurar el túnel por el cual transita la información, asegurado la privacidad e integridad de los datos, así como la autentificación de los usuarios. La IETF desarrolló IPSec utilizando criptografía de clave pública y clave simétrica. Esta tecnología utiliza las ventajas de un estándar existente, en el cual la información viaja entre dos redes sobre Internet vía IP. La información enviada mediante el uso de IP pude ser interceptada fácilmente.

El protocolo SSL habilita la seguridad en la conexión punto-punto entre dos aplicaciones; IPSec habilita la seguridad de la conexión de la red entera. Los algoritmos usados comúnmente en IPSec para el intercambio de claves son RSA y Diffie-Hellman, así como los DES o 3DES los cuales son utilizados para la encriptación. Un paquete IP es encriptado y enviado dentro de un paquete IP regular, quien es el que crea el túnel. El receptor descarta el paquete IP externo y desencripta el paquete IP interno.

La seguridad de la VPN recae en 3 conceptos: Autentificación de usuario, encriptación de los datos enviados sobre la red y el control de acceso de la información corporativa. Para ubicar estos tres conceptos, IPSec se compone de tres piezas. El Encabezado de Autentificación (AH) que agrega información adicional a cada paquete, verifica la identidad del remitente y prueba que los datos no han sido modificados. La

Carga útil de Encapsulamiento de Seguridad (ESP) encripta la información utilizando cifrado de calve simétrica para proteger los datos de los robos de señal mientras el paquete IP está siendo enviado de una computadora a otra. Finalmente, el Intercambio de Clave de Internet (IKE) que es el protocolo de intercambio de llave utilizado en IPSec para determinar las restricciones de seguridad y autentificar las claves de encriptación.

5.4.3 Virus

Los virus son piezas de códigos comúnmente enviados como archivos adjuntos u ocultos en clips de audio, video y juegos que se agregan o sobrescriben otro programa para replicarse por si mismos. Los virus pueden corromper archivos o incluso dejar inservible un disco duro. Antes que la Internet fuera inventada, los virus se esparcían a través de archivos y programas transferidos a la computadora por discos removibles. Actualmente, los virus se extienden sobre las redes simplemente compartiendo un archivo infectado incluido en un correo electrónico, documento o programa.

Existen muchas clases de virus. Un virus transitorio se adjunta a un programa específico y se activa cuando el programa al que está adherido es corrido, pero es desactivado cuando se cierra el programa. Un tipo de virus más poderoso es el virus residente, el cual una vez cargado en la memoria de la computadora opera durante el tiempo que la máquina esté en uso. Otro tipo de virus es la bomba lógica, el cual se activa cuando cierta condición se presenta. Este tipo de virus se puede activar por ejemplo cuando el reloj de la computadora concuerde con una fecha u hora exacta.

Un gusano es similar a un virus, a excepción de que éste se puede esparcir e infectar archivos por si mismo; los gusanos no requieren de estar adjuntos a un programa para esparcirse. Una vez que un virus o gusano es liberado, puede esparcirse rápidamente infectando miles de computadoras a nivel mundial en cuestión de horas o minutos.

Un caballo de Troya es un programa malicioso que se oculta en otro programa o simula la identidad de un programa legítimo mientras está causando daño a la computadora o a la red en la cual está conectado el equipo infectado. Este tipo de virus

son difíciles de detectar, debido a que suelen simular aplicaciones útiles y legítimas. Comúnmente asociados con los caballos de Troya se encuentran los programas de puerta trasera (backdoor), los cuales son virus residentes que otorgan al que envía el virus acceso completo e indetectable sobre el equipo de la víctima. Estos programas se encargan de enviar información confidencial sin importar que tan segura sea la conexión entre el servidor y el equipo infectado debido a que la información es interceptada antes de ser encriptada.

5.4.4 Firewalls

La capacidad de conectar una computadora con cualquier otra computadora es una ventaja a medas. Para los usuarios domésticos, navegar en Internet significa mucha diversión y para los gerentes de seguridad empresarial es una pesadilla. Muchas empresas tienen en línea grandes cantidades de información confidencial que si cayera en manos de un competidor podrían tener grandes consecuencias. Además de la fuga de información se encuentra la infiltración de la misma como lo son virus digitales. Debido a esto se requieren mecanismos para mantener segura nuestra información y uno de estos puede ser los Firewalls (Pared de fuego).

El propósito de un Firewall es la protección de una LAN contra intrusos fuera de ella. Un firewall actúa como una barrera segura para el flujo de información desde y hace el interior de una red de área local. Existen dos tipos de firewalls: los de filtrado de paquetes y los de compuertas de nivel de aplicación.

Los firewall de filtrado de paquetes examinan toda la información enviada desde el exterior de la LAN y automáticamente rechaza cualquier paquete que lleva una dirección de la red local. Esto es si una persona externa consigue una dirección de la red interna y desea enviar un paquete dañino a la red local interna es rechazado, debido a que el equipo externo aunque posee una dirección válida se encuentra fuera de la red LAN.

CAPITULO 6

METODO

6.1 Características del Sistema

En una red LAN cuya topología es estrella, se tienen instalados 15 equipos de cómputo los cuales cuentan con aplicaciones de Internet y otros paquetes de computación que son utilizados para impartir cursos para el manejo de los mismos. El cableado que conforma la red cumple con la normativa EIA/TIA 568, utilizando la configuración T568B de dicha norma (ver Apéndice A) para la realización de conectores macho y hembra. La velocidad de transmisión es de 100Mbps, proporcionada por un cableado UTP categoría 5.

Esta red comparte un enlace a Internet dedicado de 256Kbps. Para la navegación a Internet se tiene habilitado un servidor en el nodo donde se recibe el servicio de Internet, el equipo cuenta con un software para compartir la conexión existente de 256Kbps a los 15 equipos de la red, el nombre el software es Winproxy, cuya función principal es el filtrado de los sitios a los cuales se puede tener acceso desde los equipos de la red.

La navegación a pesar de atravesar el proxy (software) que en teoría aceleraría las consultas a Internet es muy deficiente, debido a que el equipo que funciona como

servidor es muy viejo, así también el costo de actualización de dicho equipo es muy alto, por tal motivo se está planeando eliminar este sistema y colocar un equipo ruteador.

6.2 Hipótesis

Un equipo de ruteo o ruteador es un dispositivo de red quien dentro de sus funciones básicas se encuentra la de filtrado de paquetes y unión de redes diferentes como lo son las Redes de Área Local (LAN), las Redes Inalámbricas de Área Local (WLAN) y Redes de Área Amplia (WAN); dichas funciones son más eficientes que las ofrecidas por un servidor que requiere de un software especial. La optimización del equipo ayudará a controlar el filtrado de la información que entra y sale de la red, así como agilizar la comunicación entre computadoras. Al agregar una red inalámbrica al sistema existente nos brindará la oportunidad de escalabilidad, si agregamos más equipos a la configuración actual se puede lograr sin la necesidad de incrementar costos.

6.3 Procedimiento

Se inició con el análisis del sistema instalado. El equipo que funciona como servidor proxy es una microcomputadora con las siguientes especificaciones:

- Procesador Cyrix de 300MHz
- 128Mb de memoria RAM
- Disco duro de 4.0Gb
- Tarjeta de Red (Internet) PCI 3Com 10/100 Base Tx
- Tarjeta de Red (LAN) ISA 3Com 10 Base Tx

Las computadoras que utilizan los usuarios y que conforman la red, cuentan con las siguientes características:

- Procesador Intel de 700Mhz
- 128Mb de memoria RAM
- Disco duro de 10Gb
- Tarjeta de Red Integrada 3Com 10/100 Base Tx
- Multimedia

Solo 14 equipos están conectados a un panel de parcheo. Del panel de parcheo, las 14 estaciones en conjunto con el servidor y un equipo adicional son conectados a un Hub (Concentrador) 3Com Office Connect de 16 puertos 10/100Base-TX, para de esta forma obtener la topología estrella, como se muestra en la figura 6.1.

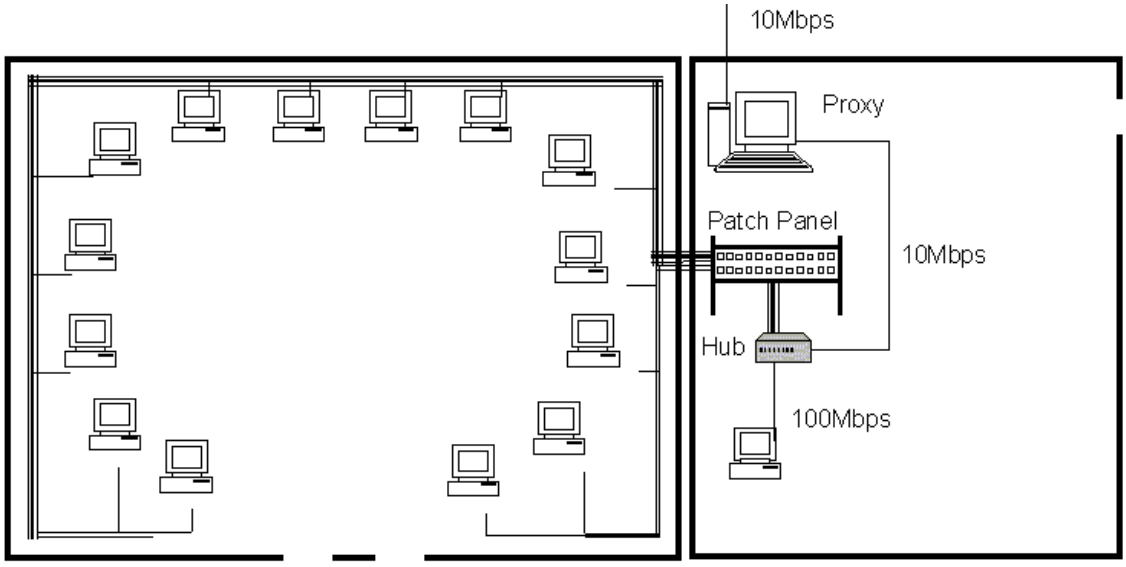


Figura 6.1 Configuración Sala

El servidor recibe la información de Internet por un cable UTP categoría 5. El servicio de Internet dedicado es proporcionado por AT&T mediante un enlace de microonda que llega a una estación receptora para posteriormente ser enviado vía fibra óptica a nuestro edificio donde un transceptor se encarga de realizar la conversión del medio fibra óptica a UTP.

Una vez analizado el hardware continuaremos con el software de la sala. La configuración actual del sistema cuenta con el uso del software winproxy corriendo sobre la plataforma Windows 98. Es importante hacer notar que el software al que se hace mención requiere de un pago anual para cubrir 25 licencias de uso, ya que el proveedor no ofrece un paquete de 15 licencias que es el ideal para nuestra configuración. La sala, cuando está en funcionamiento como sala de navegación de Internet o cursos de capacitación de otras aplicaciones diferentes a Internet, debe tener bloqueados direcciones en donde se puedan consultar correo electrónico, salones de pláticas (Chats) o cualquier otro sitio que sea considerado ofensivo, inmoral o inseguro.

Cuando se están impartiendo cursos de Internet proporcionados por el mismo proveedor de Internet no deben existir bloqueos. Los equipos que conforman la red requieren de una configuración fija, ya que el servidor proxy no realiza las funciones de asignar direcciones IP a los equipos que conforman la red.

Otra de las configuraciones que se tiene activas en el servidor proxy, es el bloqueo de los sitios de Internet con contenido inapropiado para la sala, las direcciones de Internet que estarán bloqueadas deben ser ingresadas una a una a un listado en el servidor proxy denominado "Lista negra". Es importante mencionar que dicha lista no se puede respaldar por lo que si existe una pérdida en la configuración se requiere crear nuevamente la lista manualmente.

Las estaciones de trabajo, al igual que el servidor cuentan con la plataforma Windows 98. Estas estaciones deben tener cargada la paquetería utilizada para los cursos así como la aplicación de navegación de Internet, que cuanta con un límite de tiempo para navegar de 30 minutos.

Aprovechando los beneficios de las redes LAN, todas las estaciones tienen habilitada la opción de compartir archivos e impresoras, ya que en determinados cursos es requerida la impresión y almacenamiento de información en medios externos.

Ahora se explicará brevemente el proceso en el cual estamos presentando problemas. Las dificultades se aprecian claramente a la hora en que la sala está habilitada con la navegación en Internet. El usuario toma una de las estaciones de trabajo, la cual previamente está preparada con el software para la navegación, e inicia con una pantalla en la cual se le explica brevemente las reglas de navegación. Al iniciar la navegación todas las máquinas deben arrancar sobre una página de inicio predeterminada, en la cual si el usuario no tiene idea de lo que es Internet puede utilizarlo sin problema ya que se cuentan con varios enlaces de interés general como lo son entretenimiento, noticias, educación, etc., si la persona ya tiene conocimientos sobre la navegación por Internet puede hacer uso de la barra de dirección en donde se puede ingresar la dirección a la que

se desea visitar. En el servidor proxy se tiene habilitado un espacio en disco para almacenar las páginas más visitadas y así agilizar las consultas el cual no es de gran ayuda ya que aún se aprecia un retardo considerable en el despliegue de la información solicitada en pantalla de las estaciones de trabajo. Cuando muchos usuarios desean entrar a la misma página la lentitud es mucho más evidente. Si el usuario visita una de las páginas que están configuradas como inaccesibles, no se muestra ningún mensaje en pantalla indicando que la dirección a la cual desea acceder está bloqueada y el usuario vuelve a intentar visitarla ocasionando que se levante un reporte mencionando fallas en la conexión de la sala.

Otro de las desventajas del software winproxy es que impide crear un filtrado que englobe varias direcciones, hay que ingresar específicamente cada dirección que se desea bloquear.

Una vez analizada la arquitectura y los problemas a resolver, se procede con la búsqueda del equipo de ruteo que cumpla con nuestras necesidades, las cuales se enlistan a continuación solo las más significativas:

- Bloqueo de Puertos
- Bloqueo de direcciones (URL)
- Puertos Ethernet 10/100 Base-Tx
- Puerto WAN Ethernet Base-TX o Base-FX
- Puerto para Consola
- Punto de Acceso integrado o puerto para colocar el punto de acceso para nuestra red WLAN.

Buscando entre las diversas marcas y modelos ofrecidos por los proveedores autorizados por la empresa encontramos 3 opciones que nos pueden servir para mejorar nuestra configuración de red actual. En primer lugar tenemos un equipo que consideramos de nivel avanzado en cuanto a configuración y manejo, el ruteador es de la marca Cisco Systems de la Serie 800. El modelo elegido es el 831, cuyas características

principales pueden apreciarse en el Apéndice B. En segundo lugar tenemos un equipo 3Com considerado de nivel intermedio. La familia que se eligió es la 3000, de entre los cuales se seleccionó el modelo 3012 (ver Apéndice C) y como tercera y última opción tenemos un equipo de nivel intermedio bajo, de la marca D-Link de donde se tomamos el modelo DI-624 (ver Apéndice D). De los equipos antes mencionados es importante hacer notar que solamente el último posee un punto de acceso integrado para las redes inalámbricas.

Por las características y presupuesto asignado se determinó utilizar la tercera opción para implementarse en nuestro sistema, uno de los punto claves por los que se seleccionó el equipo de la marca D-Link es que el dispositivo trae incluido el punto de acceso para la red inalámbrica y no se requiere la compra de un dispositivo externo para integrar la red WLAN a nuestro sistema. El equipo DI-624 tiene entre sus características más importantes lo siguiente:

- 4 puertos 10/100 Base-TX
- 1 puerto WAN 10 Base-TX
- Compatibilidad con los estándares 802.11 b y g para redes inalámbricas.
- Contrafuego
- Servidor DHCP
- Bloqueo de Dominios
- Filtrado de URL
- Filtrado de direcciones IP
- Interfase gráfica de configuración vía WEB

El equipo seleccionado es actualizable vía software, también cuenta con la aplicación para realizar respaldos de la configuración, para los casos de emergencia. Una vez que tenemos el equipo ruteador en nuestras manos se procede a la configuración del mismo. La manera más sencilla de configurar el equipo es mediante la interfase gráfica vía WEB por lo que necesitamos una computadora para acceder a la aplicación de configuración

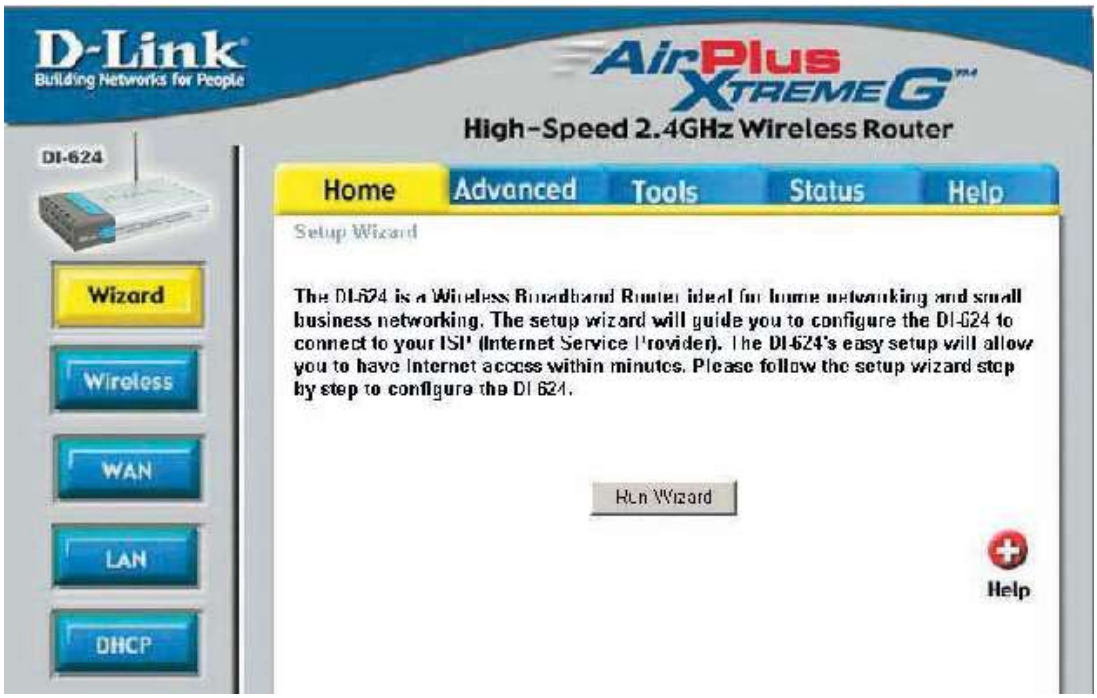


Figura 6.2 Pantalla Principal de la Configuración del Ruteador

Antes de desactivar el servidor proxy, debemos recolectar la información de la configuración que tienen las interfases de entrada y salida de este equipo, así como tener configurado completamente el ruteador. Para la configuración del puerto WAN en nuestro ruteador utilizaremos la configuración de la tarjeta de red de salida del servidor proxy. Debido a que el enlace que nos proporciona el proveedor es dedicado tenemos que ingresar la información de IP, máscara de subred, compuerta de salida y DNS a nuestro equipo de ruteo. La configuración de la tarjeta de entrada del servidor proxy no es indispensable ya que activaremos el servidor DHCP en nuestro ruteador.

Para continuar debemos tener conectada una computadora a uno de los 4 puertos del ruteador mediante un cable de red. Como mencionamos anteriormente el ruteador tiene una interfase gráfica que se puede acceder vía explorador de Internet, por lo que abrimos una ventana en nuestro navegador de Internet y tecleamos la dirección http://192.168.0.1 que es la dirección proporcionada por el fabricante para acceder a la aplicación WEB de configuración del equipo DI-624. Al ingresar por primera vez a la aplicación es necesario crear de una cuenta de usuario para la configuración y administración del equipo. Una vez creada la cuenta podemos iniciar con la

configuración básica del ruteador. En la pantalla principal (figura 6.2), podemos apreciar del lado izquierdo los botones para la configuración de nuestro equipo. La aplicación tiene un asistente (botón Wizard) para la configuración del sistema, pero en nuestro caso no haremos uso del asistente por lo que seleccionamos el botón WAN para ingresar los parámetros de configuración correspondientes para el acceso a Internet.

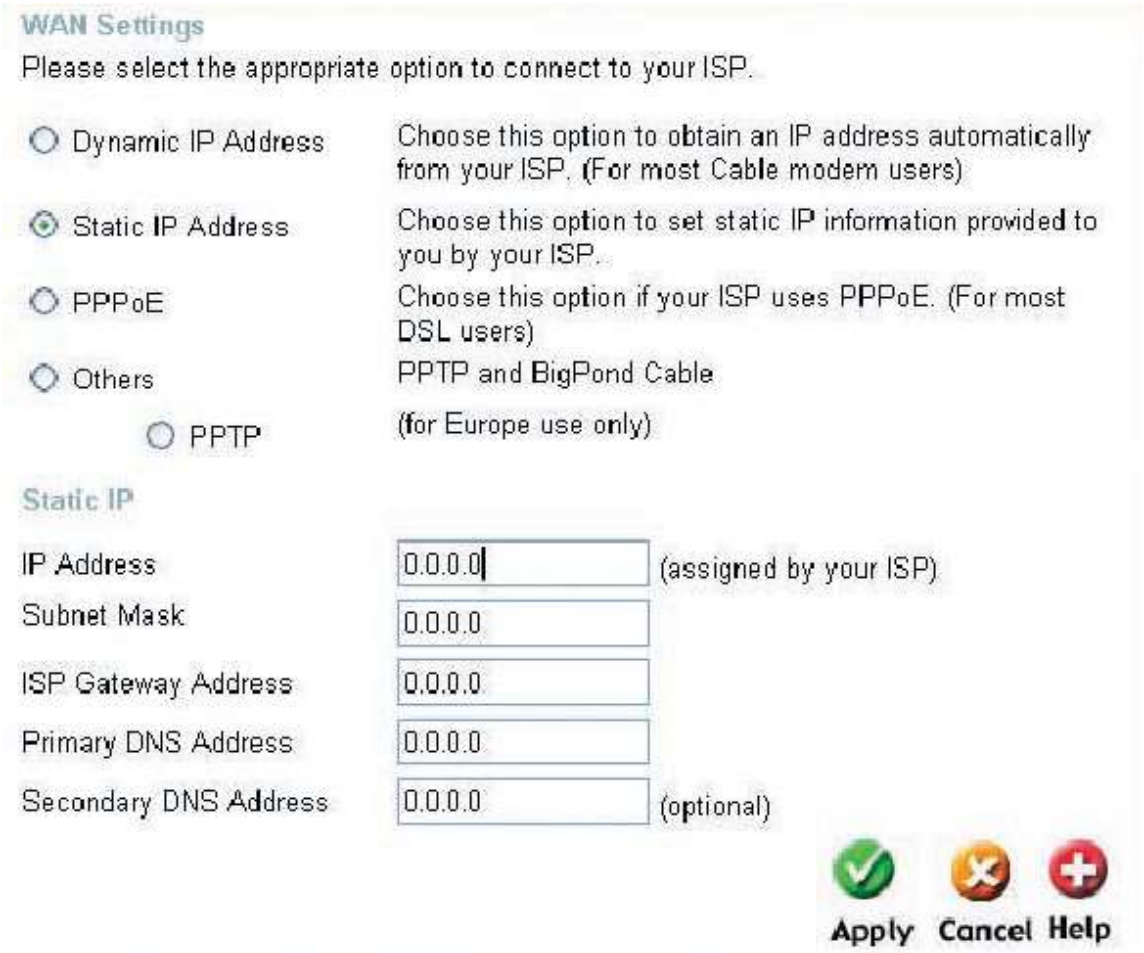


Figura 6.3 Configuración del puerto WAN

Al presionar el botón WAN apareció una ventana semejante a la mostrada en la figura 6.3. Nuestro equipo ruteador cuenta con varias formas de conexión con el proveedor de servicio de Internet (ISP), por lo que debemos estar seguros de cuál de ellas es la correcta para nuestra configuración. En nuestro caso, como mencionamos anteriormente tenemos asignada una IP estática y procedemos a la configuración de la conexión WAN utilizando la información obtenida de nuestro servidor proxy.

Terminada la configuración de nuestro puerto WAN, tuvimos que asegurarnos que el puerto está trabajando correctamente; para realizar la prueba de funcionamiento seleccionamos la pestaña “Tools” localizada en la parte superior de la pantalla, al cambiar la ventana en nuestro navegador, del lado izquierdo seleccionamos la última opción “Misc.” para que apareciera la pantalla que nos permitirá realizar la prueba de comunicación con un dispositivo externo a nuestra red LAN (figura 6.4). Temporalmente conectamos nuestro ruteador al proveedor de Internet mediante el uso del puerto WAN. Utilizamos el comando “ping”, el cual envía una pequeña cantidad de bytes para comunicarse con un equipo. Si el equipo está activo, devolverá un mensaje avisando que los paquetes fueron recibidos con éxito. Ahora en nuestro explorador, en la casilla donde aparece “Host name o IP Address” tecleamos el nombre www.yahoo.com que es una dirección IP localizada en la nube de Internet que queremos accesar. El equipo al que contactamos nos respondió favorablemente y confirmamos que la configuración del puerto WAN está correcta.

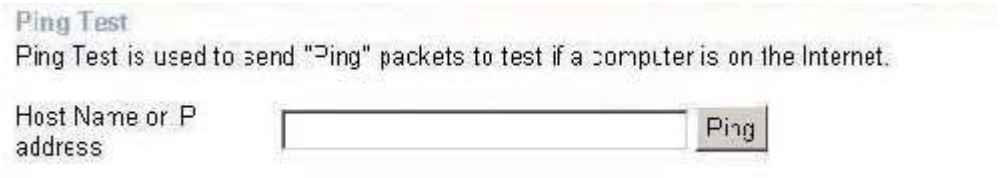


Figura 6.4 Prueba del comando ping.

Ahora procederemos con la configuración de lo que será nuestra red LAN, presionamos sobre la pestaña con el nombre de “Home” en la parte superior de la ventana en donde actualmente nos encontramos y posteriormente del lado izquierdo seleccionando el botón LAN, apareció la interfase para configurar nuestra red de área local (figura 6.5). Es en esta pantalla donde podemos configurar el ruteador para que forme parte de la red de área local ya existente en nuestra oficina o lugar de trabajo pero en nuestro caso utilizamos la información propuesta por el fabricante para crear una red nueva, ya que al retirar el servidor proxy la configuración de red LAN con la que estamos trabajando desaparecerá. Es importante documentar la configuración de nuestra red LAN para la correcta administración del sistema y escalabilidad de la misma

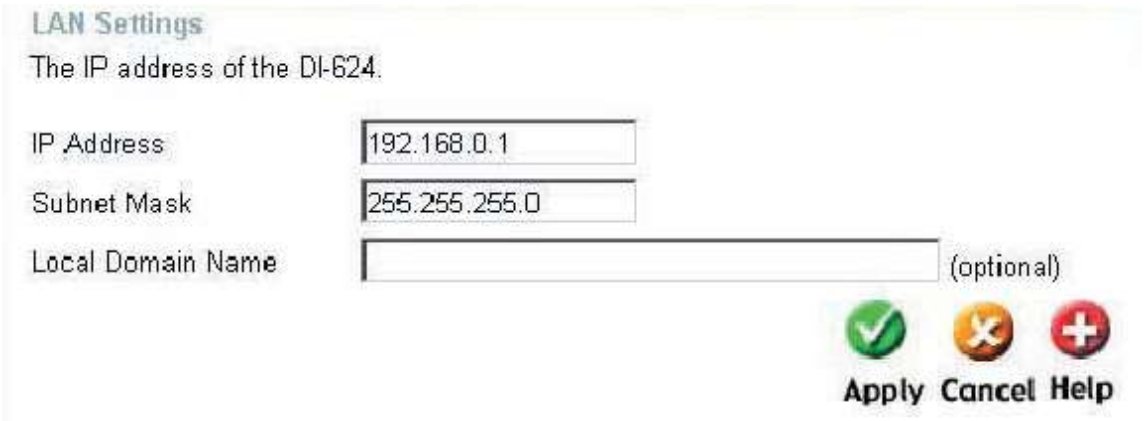


Figura 6.5 Configuración de la red LAN.

Una vez configurada la red LAN activamos el servidor DHCP, el cual evitará la tarea de configurar los equipos de los usuarios manualmente. Lo anterior se logró especificando el rango de IP que se destinará para los usuarios, la mascara de subred y la compuerta de salida que en este caso es la dirección de nuestro ruteador. Para acceder a la pantalla de configuración del servidor DHCP, presionamos el botón "DHCP" localizado al final de la columna a la izquierda de la pantalla donde configuramos la red LAN. La figura 6.6 muestra la pantalla en donde habilitamos y configuramos este servicio. Nuevamente utilizamos la información proporcionada por el fabricante. Podemos apreciar que el sistema muestra una lista de los equipos que están conectados y la IP asignada.

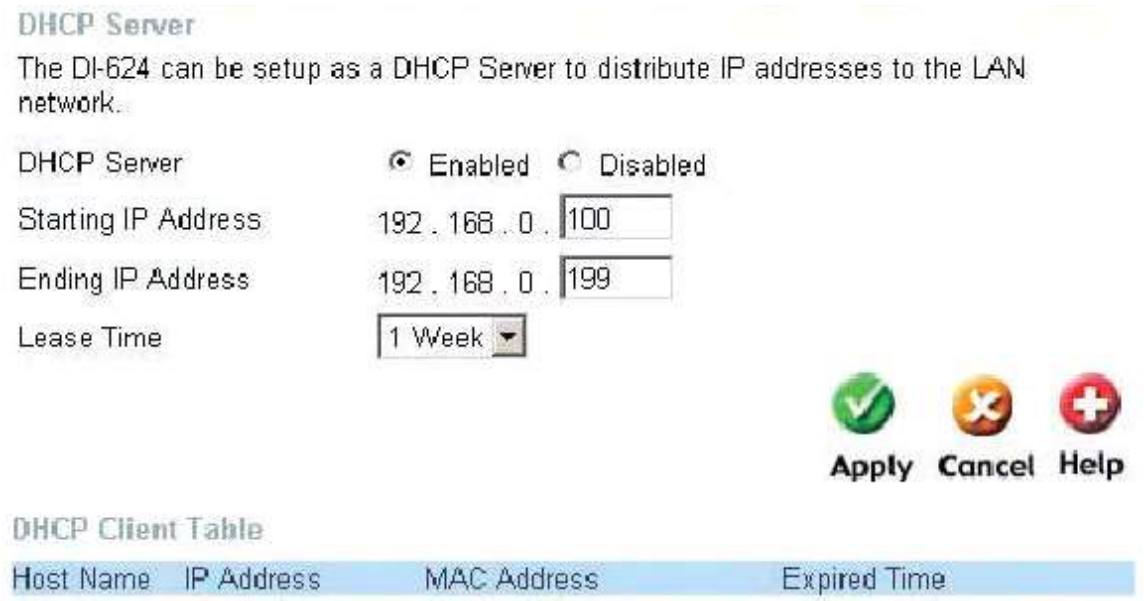


Figura 6.6 Configuración DHCP.

Continuando con la configuración del equipo de ruteo, necesitamos habilitar el puerto 80 del protocolo TCP para que los equipos puedan tener acceso a Internet, por lo tanto es indispensable la creación de un servidor virtual. En la figura 6.7 se puede apreciar la pantalla de configuración utilizada para crear el servidor virtual. Para entrar a dicha pantalla, seleccionamos la pestaña "Advanced" en la parte superior de la ventana en la que actualmente nos encontrábamos y posteriormente seleccionamos el botón "Virtual Server". Como se puede ver en la figura, tenemos la opción de restringir el acceso al servidor que estamos creando gracias a la característica de horario "Schedule", lo anterior es muy importante ya que deseamos que el servicio esté disponible únicamente en horario de oficina. Definimos nuestro horario de acceso así como los días de la semana en que se activará el servidor para terminar con la configuración. El ruteador nos permite habilitar varios servidores de servicios como FTP, DNS, HTTPS.

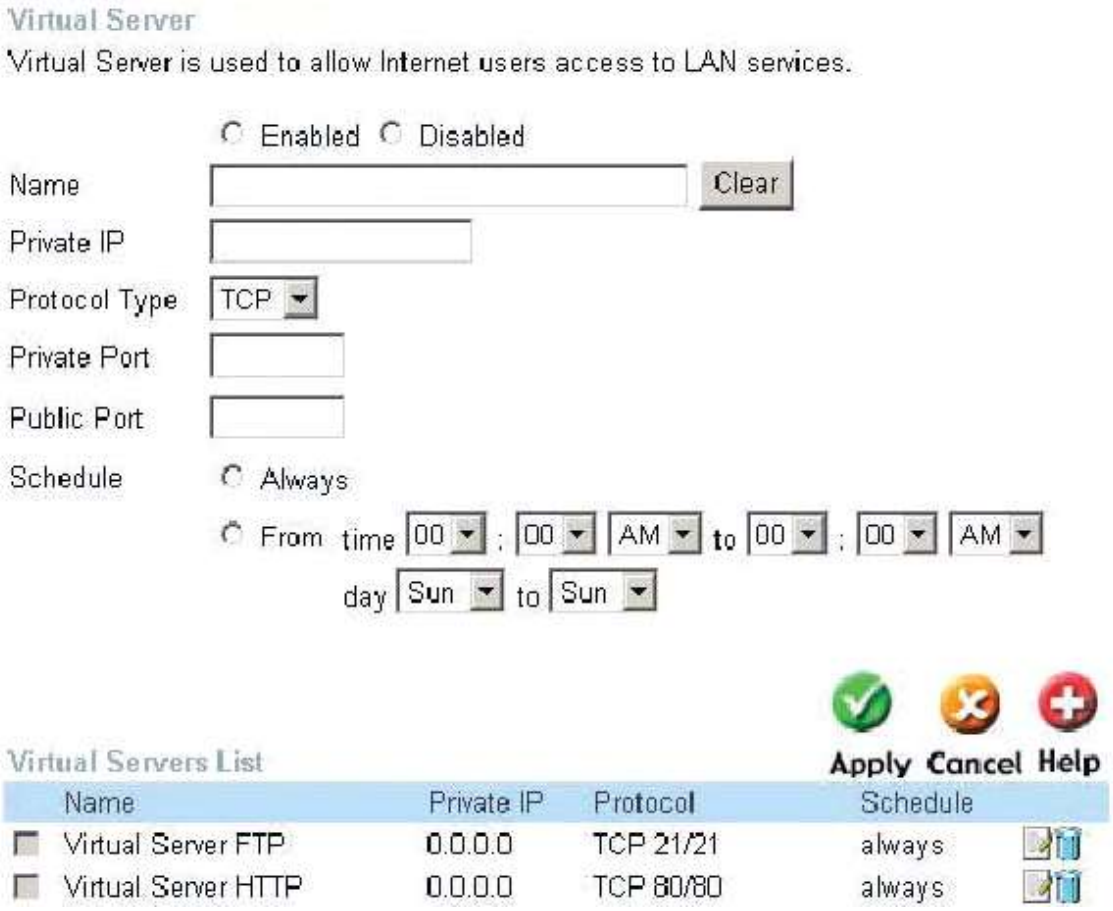


Figura 6.7 Servidor Virtual de Internet.

Terminada la configuración del servidor HTTP es de vital importancia habilitar las opciones de filtrado de contenido. El equipo de ruteo con el que estamos trabajando nos permite realizar el filtrado de contenido de 4 formas diferentes, el primero es el filtrado de IP, el segundo es por filtrado de direcciones MAC, el tercero por filtrado de direcciones URL y por último tenemos el filtrado de dominios. Basados en nuestro tipo de servicio a ofrecer, se decidió por utilizar las dos últimas opciones.

Para accesar a la pantalla de la configuración de filtrado, seleccionamos el botón "Filters" de la columna localizada a la izquierda de nuestra ventana actual. Empezaremos con el filtrado por URL (figura 6.8) el sistema proporciona una casilla en donde debemos alimentar la palabra o frase que se desea bloquear, como estamos utilizando el filtrado por URL el equipo analizará todas las direcciones introducidas por el usuario en las estaciones de trabajo y denegará el acceso a los sitios en cuya dirección URL aparezca la o las palabras que forman parte del listado en este tipo de filtrado.

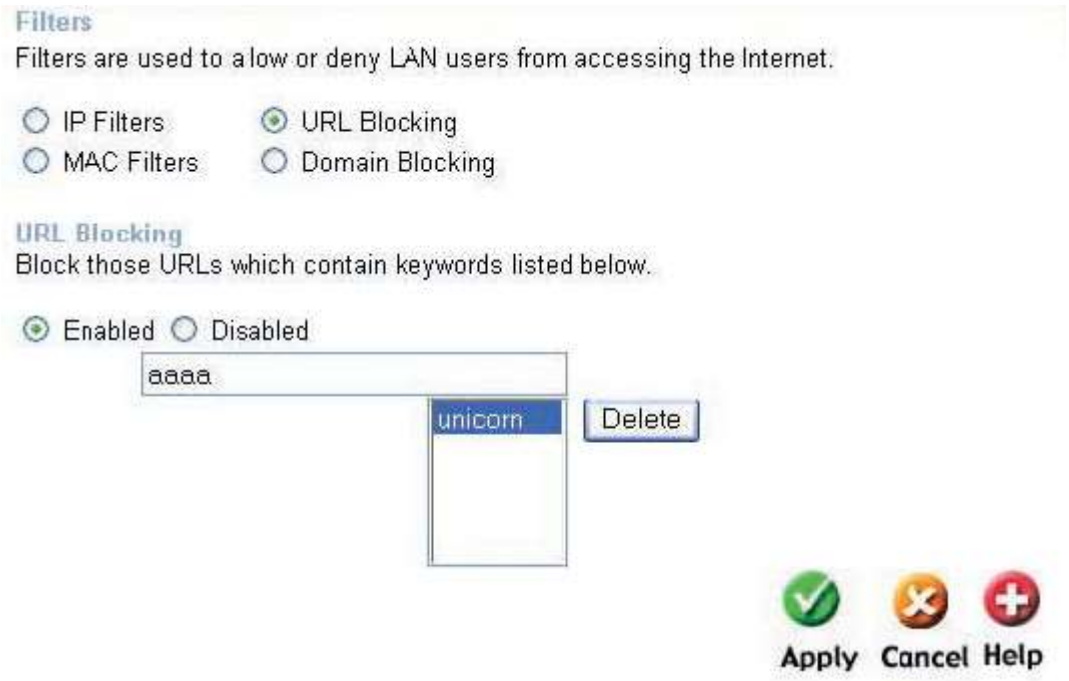


Figura 6.8 Filtrado de URL.

La ventaja del sistema DI-624 es que si se intenta ingresar a un sitio prohibido, en la pantalla del explorador de Internet aparecerá un mensaje similar al siguiente "El sitio

está bloqueado por el Administrador"; de esta forma se le hace saber al usuario que el sitio al que está intentando conectarse no está permitido. Como se mencionó en la sección 6.3 de éste capítulo, por políticas de la empresa queda prohibido el uso de sitios para la consulta de correos electrónicos, salones de pláticas o sitios cuyo contenido sea considerado ofensivo, inmoral o inseguro. Una de las limitantes del uso de este filtrado es que la lista únicamente puede almacenar diez palabras y debido a lo anterior fuimos muy cuidadosos al momento de seleccionar las palabras que conformarán la lista final del filtrado.

Para el filtrado de dominios, tuvimos que especificar la dirección de Internet tal y como lo hacemos en la barra de direcciones de nuestro explorador de Internet. El ruteador proporciona 2 listas, una en la cual se especifican los dominios a los cuales no se permitirá el acceso "Blocked Domains" y otra en la cual se listan los dominios a los cuales si tendremos acceso "Permitted Domains". La diferencia entre ambos bloqueos radica en que si elegimos la opción de utilizar la lista de dominios bloqueados, se podrá tener acceso a todos los dominios de Internet a excepción de los que conforman la lista de bloqueo y si se elige utilizar la lista de dominios permitidos, todos los dominios de Internet estarán bloqueados a excepción de los que conforman nuestra lista de direcciones permitidas. Queda a nuestra elección el método de filtrado de dominios a utilizar. Para nuestra red, utilizamos el listado de dominios bloqueados. De nueva cuenta la lista estuvo limitada a 10 dominios, por tal motivo tuvimos que considerar dominios que no quedaron bloqueados por el filtrado de direcciones URL.

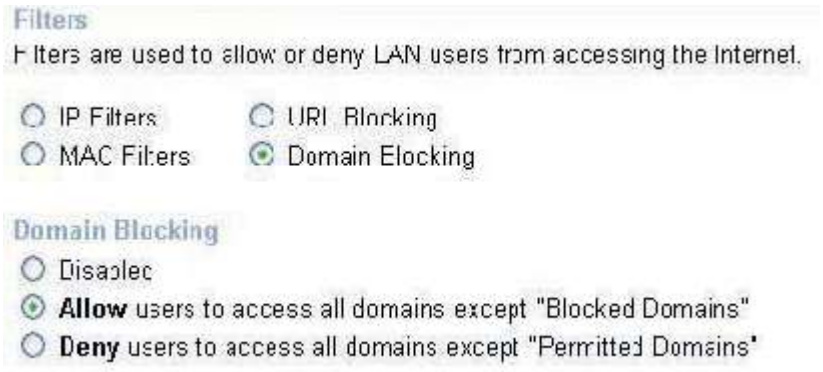


Figura 6.9 Filtrado de dominios.

Una vez que ingresamos toda la información procedimos a la verificación del sistema, para lo cual utilizamos una de las estaciones de trabajo para realizar una consulta a una dirección de Internet. Antes de proceder tuvimos que comprobar que el servidor DHCP estuviera funcionando, por lo que fue importante revisar que la estación de trabajo en la que estaremos trabajando tuviera una dirección IP, máscara de red y puerta de enlace correctas. Utilizamos el comando ipconfig en una ventana de msdos para verificar la información de nuestra tarjeta de red. Confirmada la configuración del equipo, continuamos con la prueba de acceso al servicio de Internet y revisión de las reglas de filtrado.

Para iniciar con las pruebas conectamos nuevamente el ruteador al servicio de Internet mediante el puerto WAN, dejando temporalmente al servidor proxy sin servicio de Internet pero trabajando con la red LAN. Es importante mencionar que estas pruebas se realizaron en horarios que no afectaran el trabajo cotidiano de la red que deseábamos mejorar para evitar entorpecer el trabajo de los usuarios finales. Utilizando una de las estaciones de trabajo se abrió el explorador de Internet y en la barra de direcciones tecleamos la dirección del fabricante del equipo de ruteo: www.dlink.com, como se tuvo acceso al sitio del fabricante, se comprobó que el servicio de consulta de Internet está trabajando correctamente.

Ahora pasamos a la prueba del filtrado de contenido para lo cual tecleamos la dirección www.hotmail.com en la barra de direcciones del explorador de Internet; la dirección proporcionada fue una de las direcciones que deben estar bloqueadas debido a las políticas de la empresa en la cual se está trabajando. En la computadora donde estuvimos corriendo las pruebas se apreció el mensaje de alerta indicando que el sitio que intentamos visitar está bloqueado por el administrador, debido al comportamiento anterior estamos seguros que nuestro filtrado está activo y funcionando adecuadamente. Terminadas las pruebas se desconectó el servicio de Internet en nuestro ruteador y se reactivó el servicio en el servidor proxy.

Debido a que las pruebas resultaron satisfactorias, procedimos a respaldar la configuración de nuestro equipo de ruteo, para poder levantar el servicio en caso de contingencia. Nos trasladamos a la pantalla que nos ayudó en el proceso de respaldo, dicha pantalla la pudimos encontrar presionando la pestaña "Tools" en la parte superior de la ventana actual y el botón "System" de la columna a la izquierda de la nueva pantalla; la opción para el respaldo del sistema se muestra en la figura 6.10.

Figura 6.10 Respaldo de la configuración.

En esta pantalla guardamos la configuración en el disco duro del equipo que estamos utilizando para configurar el ruteador y como copia de seguridad se almacenó nuevamente en una memoria portátil USB. Es en esta pantalla también en donde se puede mandar llamar el archivo que tenemos de respaldo en caso de que nuestro equipo pierda configuración. Una vez hecho el respaldo del ruteador, terminamos con la configuración de la red alámbrica.

Tocó el turno de configurar la red inalámbrica (WLAN), la cual se logró configurando el punto de acceso ("Access Point") que trae integrado nuestro ruteador. Para acceder a la pantalla de configuración, presionamos la pestaña "Home" en la parte superior de la pantalla y elegimos el botón de "Wireless" (figura 6.11). Iniciamos eligiendo un nombre para nuestra red conocido como SID, es el primer campo que apareció en nuestra pantalla de configuración. Como segundo campo tenemos el número

de canal por el cual estará activo nuestro servicio. También tenemos la opción de habilitar la encriptación WEP y el nivel de encriptación de 64 bits o 128 bits en nuestra red inalámbrica. Para nuestro proyecto utilizamos la configuración de fábrica para cada campo y la encriptación queda deshabilitada debido a que la arquitectura de nuestro edificio nos brinda un aislante radioeléctrico muy bueno evitando que la señal se propague hacia el exterior.

Es importante hacer notar que las tarjetas de red inalámbricas detectan la presencia de una red WLAN mediante el SID irradiado por el punto de acceso y si dicha red no tiene la seguridad activada, el equipo que posee la tarjeta de red inalámbrica podrá entrar a la red sin problemas.

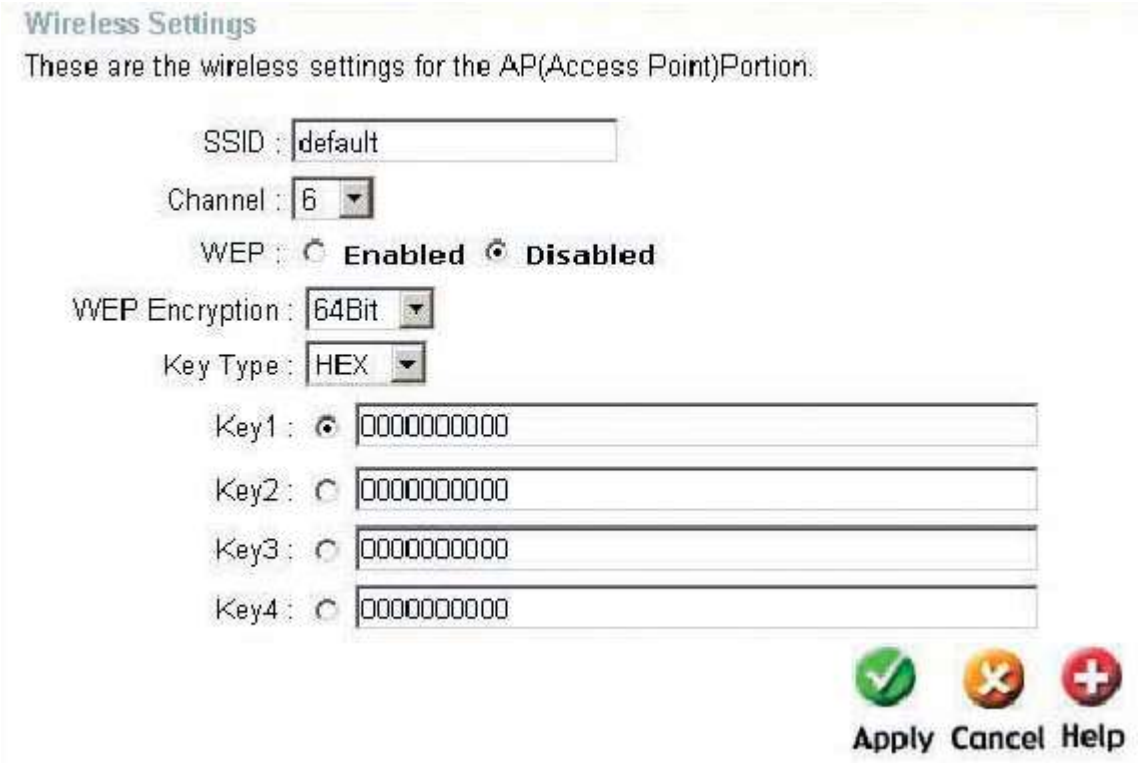


Figura 6.11 Configuración WLAN.

Para comprobar el funcionamiento de la red inalámbrica, tomamos un equipo portátil con tarjeta de red inalámbrica y lo encendimos. Las características del equipo utilizado en este proyecto son las siguientes:

- Computadora portátil Sony VAIO modelo PCG-FXA678
- Procesador AMD de 1Ghz,
- Memoria RAM de 256MB
- Tarjeta de red inalámbrica D-Link Air Plus modelo DWL-G650.

Volvimos a conectar temporalmente el servicio de Internet a nuestro ruteador. Al encender la computadora portátil con la tarjeta de red inalámbrica activada, el sistema operativo del equipo portátil indicó que localizó una red inalámbrica cercana al sitio en donde nos encontramos y como sabemos que la red inalámbrica de nuestro proyecto carece de seguridad fue muy sencillo formar parte de la red inalámbrica ya que el servidor DHCP también trabaja para la red inalámbrica. Estando dentro de la red inalámbrica procedimos a consultar una dirección de Internet válida, nuevamente tuvimos éxito en nuestra consulta. En este punto tenemos la certeza de que el sistema inalámbrico agregado a nuestra red de área local funcionó correctamente.

Respaldamos la configuración de nuestro ruteador una vez más, ya que ahora tenemos configurada la red inalámbrica y la red alámbrica.

CAPITULO 7

RESULTADOS Y CONCLUSIONES

7.1 Resultados

Después de haber reemplazado el servidor proxy por el ruteador D-Link modelo DI-624 y trabajado con la nueva configuración de la red de área local por espacio de 30 días, no encontramos incidentes que indicasen deficiencia en el desempeño de la red.

En la figura 7.1 se puede apreciar la configuración final de nuestro sistema, el cual se puede comparar con la figura 6.1 para identificar los cambios aplicados a la configuración inicial de nuestra red de área local.

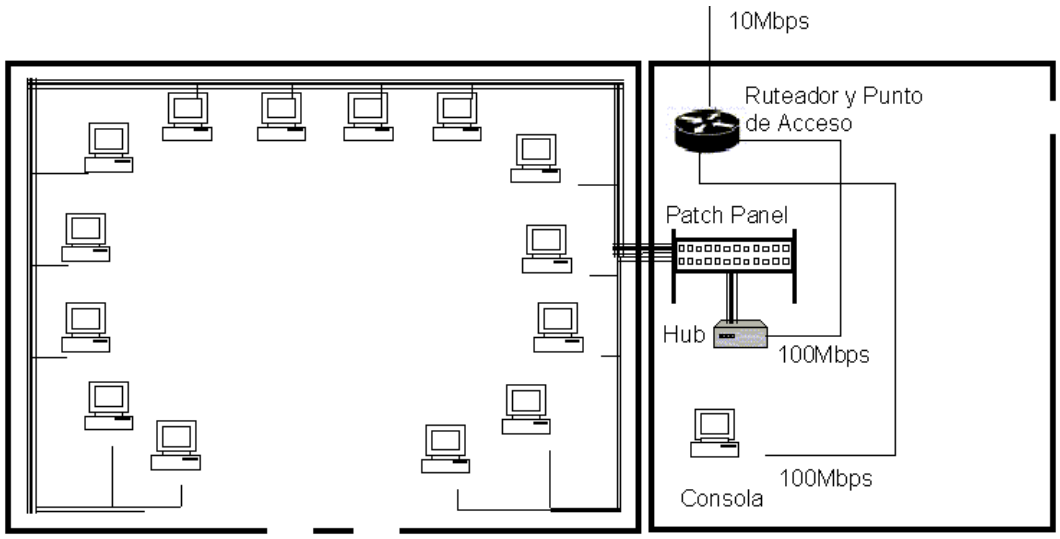


Figura 7.1 Configuración final de la Sala.

7.1.1 Ventajas y Desventajas del Ruteador

La colocación del ruteador para sustituir las funciones del servidor proxy, se realizó con éxito. No se presentaron problemas graves en cuanto a la configuración y su funcionamiento es mucho mejor que el proporcionado por servidor, entre las ventajas de colocar un ruteador en nuestro sistema encontramos las siguientes:

- ✓ La interfase para el manejo del ruteador que se eligió es gráfica y por tal motivo su configuración es muy sencilla y amigable.
- ✓ Se tiene la ventaja de generar respaldos de nuestras configuraciones para casos de emergencia.
- ✓ El tiempo de recuperación de nuestro sistema en caso de presentarse una falla eléctrica es mucho más rápido y eficiente ya que no depende de un sistema operativo externo.
- ✓ Al contar con un ruteador con punto de acceso para las redes inalámbricas nos ahorra el problema de buscar y configurar un equipo externo para crear una red inalámbrica.
- ✓ No se requiere de pagar licencias para trabajar con el equipo en nuestro ambiente de trabajo.
- ✓ Reducción en el consumo de energía, debido a que el equipo consume menos energía eléctrica que un servidor de cómputo.
- ✓ La administración del equipo se puede realizar de manera remota.

Dentro de las desventajas que se tiene al utilizar el ruteador en nuestra configuración de red encontramos lo siguiente:

- × Se debe instalar un programa antivirus en cada equipo de nuestra red, para evitar ataques de virus.
- × Para el filtrado, solamente se tiene un máximo de 10 términos por opción de filtrado, lo anterior es debido a que el sistema de filtrado utilizado por el equipo es por hardware y no se puede actualizar.

- × Debido a la estructura de nuestro edificio, la distancia a la cual tenemos una buena señal de recepción para las tarjetas de red inalámbricas es de aproximadamente 15 mts. desde el punto de acceso.
- × Si llegaran a descubrir la contraseña necesaria para acceder al equipo remotamente, se podría causar mucho daño.

7.1.2 Ventajas y Desventajas del Servidor Proxy

El manejar un servidor proxy para compartir el enlace de Internet en nuestra red nos ofrece las siguientes ventajas con respecto al ruteador:

- ✓ Se tiene la posibilidad de monitorear en tiempo real los sitios visitados y en caso de encontrar uno no apropiado se puede terminar la sesión del usuario.
- ✓ Se cuenta con un antivirus limitado que bloquea algunos de los virus existentes.
- ✓ Nadie puede acceder el equipo si no está autorizado, debido a que las modificaciones no se pueden realizar de manera remota.

En cuanto a las desventajas que encontramos al emplear el servidor en nuestro sistema tenemos:

- × El filtrado del contenido debe ser especificado en una lista, la cual debe tener correctamente escrito el sitio a bloquear.
- × Al surgir fallas en la alimentación eléctrica, siempre es necesaria la intervención del personal de sistemas para levantar nuevamente el servicio.
- × No se pueden realizar respaldos de la configuración de la aplicación Winproxy.
- × Se requiere de un pago anual de licencias para el manejo del software Winproxy.
- × Se ocupan 2 tarjetas de red para completar la configuración del servidor, una de las tarjetas es la interfase de salida y la otra la interfase de entrada.
- × Se tiene mayor consumo de energía, ya que se utiliza una computadora en la cual se tiene grabado un sistema operativo y software Winproxy.
- × Es necesario el pago de una licencia para el uso del sistema operativo que está corriendo en la computadora donde tenemos instalada la aplicación.

7.2 Conclusiones

Los cambios realizados en los equipos de comunicaciones que son utilizados para la comunicación entre diferentes redes son muy delicados, ya que una mala planeación nos puede llevar a una deficiente configuración y por tanto una falla en nuestra red y todos sus servicios, es por eso que se debe tener mucho cuidado al momento de elegir el equipo a sustituir, así como el tiempo aproximado para realizar los cambios, configuraciones y pruebas correspondientes para que en caso de contingencia podamos revisar y resolver la falla lo más pronto posible sin perjudicar al usuario final o en casos extremos regresar al sistema anterior.

Las funciones que realiza un servidor proxy pueden ser realizadas también por un equipo ruteador, pero se debe destacar que dependiendo del tipo de actividad que se tenga en la red a modificar debemos seleccionar el tipo de ruteador a instalar. Existen equipos en el mercado que nos proporcionan muchas características como servidor DHCP, Filtrado de contenidos, interconexión con redes LAN, WAN, ATM, Frame Relay, encriptación de información, VPNs, entre otras. Nuestra decisión final debe tomar en cuenta el nivel de tráfico que manejaremos, la eficiencia, seguridad y servicios que se desean tener en nuestra red. Además se debe prever la opción de actualización de los equipos, ya que hoy en día la tecnología avanza a pasos agigantados y rápidamente la nueva tecnología queda obsoleta.

Las redes inalámbricas son de gran ayuda para la configuración de la extensión de una red alámbrica en un edificio, ya que nos ahorra mucho tiempo y capital al momento de realizar la instalación. Hay que tomar muy en cuenta la seguridad de una red inalámbrica, ya que de ello depende la confiabilidad y funcionamiento de todo nuestro sistema.

BIBLIOGRAFIA

Stallings, William,
"Data and Computer Communications",
Prentice Hall,
Fifth Edition,
1997

Tanenbaum, Andrew S.,
"Redes de Computadoras",
Prentice Hall,
Cuarta Edición,
2003

Deitel, Harvey M.
"Wireless Internet & Mobile Business, How to Program"
Prentice Hall,
First Edition
2001

Cisco Systems, Inc
"Academia de Networking de Cisco Systems: Guía del Primer Año"
Pearson Educación
Segunda Edición
2003

LISTADO DE FIGURAS

APENDICES

APENDICE A
Estándar de Cableado EIA/TIA 568

El estándar más conocido de cableado estructurado está definido por la EIA/TIA [Electronics Industries Association/Telecomunications Industries Association] de Estados Unidos, y especifica el cableado estructurado sobre cable de par trenzado UTP de categoría 5, el estándar 568A. Existe otro estándar producido por AT&T muchos antes de que la EIA/TIA fuera creada en 1985, el 258A, pero ahora conocido bajo el nombre de EIA/TIA 568B. En el mundo de los sistemas de cableado estructurado el número críptico 568 al orden en que los hilos individuales dentro del cable CAT 5 están terminados. Los elementos del sistema de cableado incluyen:

- El Cableado Horizontal
- El Cableado de "Backbone"
- El área de Trabajo
- Los Armarios de Telecomunicaciones
- Las Salas de Equipo.
- Los Puntos de Administración
- La Infraestructura de Entrada.

Las distancias máximas de cable especificadas por el estándar EIA/TIA 568 para UTP en topología estrella se indican a continuación:

- Cableado Horizontal: 90m (300 pies)
- Cableado de "Backbone": 800m (2,625 pies)
- Área de Trabajo: 3m (10 pies)
- Armarios de Telecomunicaciones
  Terminación de horizontal: 7m (23 pies)
  De Horizontal al "Backbone": 6m (20 pies)
- Sala de Equipos: 20 m (66 pies)
- Puntos de Administración

Conexión Cruzada Principal (MC): 20m (66 pies)

Conexión Cruzada Intermedia (IC): 20m (66 pies)

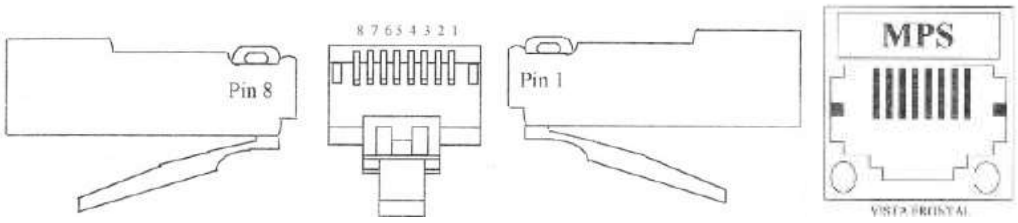
Para el estándar EAI/TIA 568 se reconocen los siguientes tipos de medios para el cableado a utilizar:

1.- Cable UTP de 4 pares y 100 ohms, calibre 24

2.- Cable STP de 2 pares y 150 ohms.

3.- Fibra Óptica de 62.5/125 micrómetros.

La configuración de los conectores macho y hembra se muestran a continuación, diferenciando entre T568A y T568B.



Conector Macho **Conector Hembra**

Figura A1. Conectores Macho y Hembra RJ45

	Macho		**Hembra**	
	T568A	**T568B**	**T568A**	**T568B**
Cable	**Pin**	**Pin**	**Pin**	**Pin**
Blanco/Naranja	3	1	3	1
Naranja	6	2	6	2
Blanco/Verde	1	3	1	3
Azul	4	4	4	4
Blanco Azul	5	5	5	5
Verde	2	6	2	6
Blanco/Café	7	7	7	7
Café	8	8	8	8

Figura A2. Configuración de los cables según el estándar EIA/TIA

APENDICE B
Ruteador Cisco modelo 831

El ruteador Cisco 831 puede conectar un teleconmutador o una pequeña oficina a un proveedor de Internet (ISP) con conexión de banda ancha o Ethernet a los siguientes lugares:

- LAN Corporativa
- Internet

El ruteador Cisco 831 tienen capacidad de switcheo y proveen 4 puertos Ethernet switcheados para una LAN. Estos ruteadores son capaces de puenteo y ruteo multiprotocolo entre los puertos LAN y WAN.

Este ruteador soporta encriptación de alta velocidad, switcheo 10/100Mbps y funcionalidad de marcación de respaldo mediante el puerto auxiliar para una consola. La función de autosensado en los puertos del ruteador, elimina la necesidad de un cable cruzado y permite a los ruteadores detectar el medio identificando si se encuentra en modo normal (MDI) o en modo cruzado (MDIX) y configurar el puerto automáticamente para lograr la comunicación.

La función de marcación de respaldo permite al usuario conectar un modem analógico al puerto para consola como un enlace de respaldo para la WAN en el caso de que el servicio ADSL tenga fallas. Estas características dan al ruteador Cisco 831 un alto nivel de seguridad y desempeño. Algunas de las características principales se encuentran enumeradas en la tabla A1. El ruteador Cisco 831 está diseñado con encriptación basada en hardware. Este ruteador permite el incremento de memoria Falsh o SDRAM.

Figura B1. Ruteador Cisco 831

Características del Ruteador Cisco 831

Características	Descripción
Puertos 10BASE-T/100BASE-T	Conexión 10/100BASE-T (10/100-Mbps) en redes Ethernet. Compatible con equipos 10/100-Mbps.
Puerto WAN	Conexión 10BASE-T. Compatible con equipos 10Mbps. Puede ser conectado a otros dispositivos de red, como módems de cable, ADSL, y ruteadores.
Memoria Flash	8 MB de memoria Flash; expandible a 16 MB de memoria Flash.
RAM Dinámica Síncrona (SDRAM)	32 MB de SDRAM en tarjeta.
Fácil Instalación	Código de color en puertos y cables, para reducir errores de instalación.
Software Cisco IOS	Soporta software Cisco IOS
Aplicación para la configuración del Ruteador Cisco.	Herramienta basada en Internet para la configuración básica y aplicaciones especiales.
Puerto para Consola	Posee una conexión para conectar una terminal o una PC para configuración de software o resolver problemas utilizando la interfaz de línea de comando.
Capacidad para el montaje en pared	Brackets en la parte inferior del ruteador para montaje en paredes o superficies verticales.
Hardware Acelerador IPSec	Solo el ruteador Cisco 831soporta esta característica. El procesador de seguridad Hifn 7902 implementa encriptación de llave simétrica, encriptación de llave pública, autentificación y compresión de información en hardware. Los algoritmos implementados por el procesador incluyen DES y 3DES; SHA-1, MD5, HMAC; y compresión LZS, MPPC.

APENDICE C
Ruteador 3Com modelo 3012

Los ruteadores 3Com Router 3012 dedicados para el acceso WAN en oficinas remotas, proporciona ruteo de acceso a WAN de alto rendimiento efectivo frente a costo, en una plataforma de escritorio. Integrado sin discontinuidades con sus equipos legacy o como parte de una solución 3Com de extremo a extremo, este ruteador ofrece procesadores de alta velocidad, calidad de servicio avanzada, soporte integrado para convergencia de voz, datos y vídeo, así como las últimas características de seguridad y control para garantizar una operación de red eficiente y segura.

- **Puertos:** Uno 10/100BASE-T; dos serie (Sínc/Asínc); uno de Consola; y uno serie AUX

- **Routing de WAN:** Frame Relay, X.21, X.25, PPP, PPPoE, MP, SLIP, HDLC/SDLC, Línea Alquilada, Sínc /Asínc, Ethernet, IP, IPX, OSPF, RIP v1/v2, BGP-4, Routing Estático

- **Seguridad:** VPN (L2TP, GRE, IPSec), Firewall, ACLs, NAT, RADIUS, PAP/CHAP

- **Convergencia:** QoS (CAR, LAR, FIFO, GTS, PQ, CQ, WFQ, RED, WRED, LLQ), Multicast (IGMP, PIM-SM, PIM-DM), VLAN 802.1q, Routing Inter-VLAN, Multilinks, Compresión

- **Resistencia ante Fallos:** VRRP (Protocolo de Redundancia de Ruteo Virtual), Centro de Backup (Configuración / Puerto), Centro de Control de Discado, Multilink

- **Administración de dispositivos:** Para una mejor administración gráfica con funcionalidades extendidas, se recomienda utilizar el 3Com Switch Manager,

cuya adquisición está disponible con 3Com Network Administrator o 3Com Network Director. Para redes más pequeñas, se puede administrar el switch de forma gráfica con el 3Com Network Supervisor. Con el dispositivo se incluyen de serie la administración mediante CLI, Telnet, puerto de consola, marcación por módem y SNMP.

- **SDRAM:** 64 MB
- **Flash:** 8 MB
- **Dimensiones:** Altura: 36,5 mm (1,47") Anchura: 251,0 mm (9,881") Fondo: 187,0 mm (7,36")
- **Peso:** 0,85 kg (1,87 libras)
- **Tensión de Entrada:** De 90 a 240 VAC
- **Consumo Máximo de Potencia:** 40W

Figura C1. Ruteador 3Com 3012

APENDICE D
Ruteador D-Link Air Plus Xtreme G inalámbrico, modelo DI-64 Revisión C.

Figura D1. Ruteador D-Link DI-624

El ruteador D-Link AirPlus Xtreme G es un punto de acceso inalámbrico a 2.4GHz basado en la tecnología 802.11g. El dispositivo está dotado de seguras funciones firewall y de (4) puertos 10/100Mbps con funciones de reconocimiento automático de la velocidad. El equipo permite a los usuarios compartir carpetas, accesos a Internet y periféricos, así también puede ser configurado fácilmente y administrado mediante un sencillo programa de configuración asistida y una útil interfaz basada en Web.

Servidor DHCP integrado

El dispositivo D-Link AirPlus Xtreme G DI-624 incorpora un servidor DHCP que, tras haber sido activado, asigna automáticamente las direcciones IP a los clientes inalámbricos de la red, con lo que se simplifica el acceso a la red local y a Internet para todos los equipos conectados. El dispositivo DI-624 dispone de una antena omnidireccional caracterizada por prestaciones superiores, y está dotado de LED de enlace status/activity que simplifican las tareas de diagnóstico.

Firewall

El equipo DI-624 protege la red mediante sofisticadas funciones firewall, fácilmente configurables en la sección "Advanced features" del programa de configuración basado en Web. El aparato está dotado de una CPU con altas prestaciones y, por consiguiente, soporta avanzadas funcionalidades de autenticación de las direcciones MAC, Stateful

Packet Inspection (SPI) y Content Filtering. Las funcionalidades avanzadas de registro y de filtrado proporcionan información sobre posibles intrusiones, y permiten la aplicación de contramedidas adecuadas. El DI-624 también soporta la función básica de control para el bloqueo de URL y dominios y el filtrado de las direcciones IP. El bloqueo URL permite impedir el acceso a sitios web con nombres de dominio que contengan determinadas palabras. El bloqueo del dominio permite impedir el acceso a determinados sitios web cualquier otro sitio relacionado. El filtrado de las direcciones IP permite impedir el acceso a determinadas direcciones IP incluso si el URL está modificado.

VPN pass-through/multisesiones:

- PPTP
- L2TP
- IPSec

Características

- Velocidades de transmisión de hasta 108Mbps
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g
- 4 puertos 10/100Mbps
- Funciones de Firewall, DMZ, VPN Pass-thru, Control de Acceso a Internet
- WPA, 802.1x
- Alimentación externa, fuente de alimentación de DC 5V, 2.0A.

ACRONIMOS

ATM	Modo de Transferencia Asíncrona
AAL	Capa de Adaptación ATM
ARQ	Petición de Repetición Automática
CIR	Velocidad Media de Transmisión
CRC	Código de Redundancia Cíclica
CSMA/CD	Acceso Múltiple con Detección de Portadora y Detección de Colisión
DHCP	Protocolo de Configuración de Host Dinámico
EIA	Alianza de Industrias Electrónicas
FDM	Multiplexión por División de Frecuencia
HF	Alta Frecuencia
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IP	Protocolo de Internet
ISM	Banda de Aplicaciones Industriales, Científicas y Médicas.
ISO	Organización de Estándares Internacional
LAN	Red de Área Local
LF	Baja Frecuencia
MAC	Control de Acceso al Medio
MAN	Red de Área Metropolitana
MDI	Interfaz Dependiente del Medio
MDIX	Interfaz Dependiente del Medio Cruzado
MF	Frecuencia Media
NAT	Traducción de Direcciones de Red
NRZI	No Retorno a Cero Invertido
NRZL	No Retorno a Nivel Cero
OFDM	Multiplexión por División de Frecuencias Ortogonales
OSI	Interconexión de Sistemas Abiertos
PVC	Circuito Virtual Permanente
SSL	Capa de Socket Seguro
TCP	Protocolo de Control de Transmisión

TDM	Multiplexión por División de Tiempo
TIA	Asociación de Industrias de Telecomunicaciones
UDP	Protocolo de Datagrama de Usuario
URL	Localizador Universal de Recursos
VHF	Frecuencia muy Alta
VLF	Frecuencia muy Baja
VPN	Red Privada Virtual
WAN	Redes de Área Extendida
WLAN	Redes de Área Local Inalámbrica