UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

CONSIDERACIONES BÁSICAS PARA EL ANÁLISIS, DISEÑO E IMPLANTACIÓN DE UN SISTEMA SEGURO DE TRANSMISIÓN DE DATOS

TESIS PROFESIONAL QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

JOEL MEJÍA RESCALVO

ASESOR:
M. EN I. GRACIELA BRIBIESCA CORREA

MÉXICO, D. F. 2002

PAGINACION DISCONTINUA

TESIS CON
FALLA DE ORIGEN

Agradecimientos

En primer lugar me gustaría dar las gracias a **Dios** por haberme dado la oportunidad de estudiar una carrera universitaria.

Asimismo quiero agradecerle a la **Universidad Nacional Autónoma de México** (UNAM) por haberme abierto sus puertas y brindarme todo el conocimiento científico y humano durante toda mi estancia en sus aulas.

También le agradezco a todas las instituciones Universitarias que contribuyeron a mi formación profesional:

- A la **Facultad de Contaduría y Administración** (FCA), en donde curse la carrera de Informática.
- A la **Dirección de Cómputo para la Administración Académica** (DCAA), por haber sido el complemento ideal para mi formación y por haberme dado la oportunidad de conocer a gente muy valiosa.
- Al **Centro de Enseñanza de Lenguas Extranjeras** (CELE), que me dio la oportunidad de estudiar el idioma inglés que será muy importante en mi vida profesional.
- A la **Dirección General de Servicios de Cómputo Académico** (DGSCA) por haberme inspirado a realizar este trabajo y enseñarme cosas nuevas y complementarias a mi formación y darme la oportunidad de poner en práctica mis conocimientos.
- A la **División de Educación Continua de la Facultad de Psicología** (DEC-Psicología), por permitirme practicar los conocimientos aprendidos en las aulas.

Muy especialmente quiero darle las gracias a mis **amigos, familiares** y **profesores** que con su apoyo y enseñanzas contribuyeron a la realización de este proyecto, que culmina una parte muy importante de mi vida.

De todo corazón ¡**GRACIAS**!

"POR MI RAZA HABLARA EL ESPIRITU"

JOEL MEJÍA RESCALVO

B

Índice

Introducción

En la actualidad la seguridad informática ha cobrado una importancia sustancial para el sector empresarial, ya que la información que se maneja muchas veces representa una ventaja competitiva o una desventaja si se carece de datos precisos y confiables. Por tal motivo es fundamental proteger la información que se maneja al interior de la organización de las amenazas y vulnerabilidades existentes al momento de su generación o en el intercambio de datos relevantes a través del sistema de comunicaciones de datos.

A pesar de la necesidad de proteger los datos confidenciales muchas empresas no cuentan con los mecanismos de protección adecuados para ello e inclusive no tienen una infraestructura de telecomunicaciones que les permita ser más eficientes y competitivos con otras instituciones y así mantener una comunicación óptima con sus socios y clientes.

Asimismo el avance tecnológico ha propiciado la necesidad de contar con una buena infraestructura de comunicaciones para poder realizar un intercambio seguro de información, por lo que este trabajo trata de puntualizar los factores clave que influyen en el proceso de la transmisión de datos y la manera en que estos se pueden proteger para garantizar su integridad y el valor intrínseco de la información. No trata de ser de ninguna manera una receta de cocina para la implantación de redes corporativas seguras, puesto que en cada caso se deben analizar los factores específicos que afectarán directamente el desempeño de las mismas. Simplemente se trata de dar una visión global de los elementos básicos que se deben tomar en cuenta al momento de diseñar una red corporativa con un grado de seguridad aceptable.

Este trabajo "*Consideraciones Básicas para el Análisis, Diseño e Implantación de un Sistema Seguro de Transmisión de Datos*" consta de 6 capítulos, los cuales se encuentran divididos en dos secciones; la primera de ellas (capítulos 1 – 3) se enfoca principalmente en la descripción de los componentes de un sistema de comunicaciones de datos incluyendo los medios físicos de transmisión y las tecnologías LAN y WAN más importantes en la actualidad. La segunda sección (capítulos 4 – 5) se orienta a la descripción de los mecanismos de seguridad que pueden ser implantados en el sistema de comunicaciones. Finalmente en el capítulo 6 se presentan algunas recomendaciones para establecer un sistema de comunicaciones con un grado de seguridad aceptable.

En el capítulo 1 "*Introducción a las Comunicaciones de Datos*" se detallan algunos conceptos básicos utilizados en las telecomunicaciones, así como una breve reseña histórica de la evolución de las comunicaciones, ya que considero que es importante tener las bases teóricas para entender con mayor claridad el funcionamiento de las diversas tecnologías de

interconexión de redes.

El capítulo 2 "*Medios de Transmisión de Datos*" describe las características principales, así como las posibles aplicaciones de los diversos medios de transmisión para la implantación física del diseño conceptual de la red corporativa, con el fin de tener una visión más clara de todas las posibilidades existentes y hacer una mejor evaluación al momento de tomar la decisión del medio de transmisión que se utilizará.

En el capítulo 3 "*Tecnologías de Interconectividad de Redes*" se señala otro punto importante al momento de diseñar una red corporativa: la elección de la tecnología de interconexión que se utilizará tanto para la red local (LAN), como para la red externa (WAN), puesto que de esta decisión dependerá en gran medida el funcionamiento de la organización. Así pues se describe el funcionamiento de las tecnologías LAN y WAN más populares para comprender la manera en que se realiza la transmisión de la información en cada una de ellas y contar con bases más sólidas al momento de seleccionar la tecnología LAN y WAN a implantar.

El capítulo 4 "*Fundamentos de Seguridad en los Sistemas de Cómputo*" describe algunos conceptos importantes relacionados con la seguridad de los sistemas de cómputo en general, así como las vulnerabilidades, amenazas y ataques a las que está expuesta la información, ya que debemos tener muy en claro cuales son los factores que afectan directamente la integridad y confiabilidad de los datos, con el fin de implantar un mecanismo de seguridad adecuado que ayude a resolver la mayoría de los huecos de seguridad existentes en la organización y garantizar la veracidad de la información.

En el capítulo 5 "*Mecanismos de Protección de la Información*" se menciona brevemente la evolución de la criptología y se analizan las técnicas de cifrado más populares hasta nuestros días, que incluyen la criptografía simétrica y la criptografía asimétrica, describiendo los algoritmos principales de cada técnica. Asimismo se describen dos técnicas criptográficas más, utilizadas en las comunicaciones, que son: el cifrado de enlace y el cifrado extremo a extremo. Además se analizan algunas herramientas de seguridad para proteger el acceso a los recursos informáticos de la organización, entre ellas el uso de NAT, firewalls y listas de acceso en los dispositivos de comunicaciones. Conociendo estas técnicas y herramientas se puede determinar con mayor precisión la estrategia más adecuada para proteger la información.

Finalmente el capítulo 6 "*Esquema Seguro la Transmisión de Información*" trata de sintetizar los elementos clave para la instalación de un sistema seguro de comunicaciones de datos proporcionando algunos consejos prácticos para el diseño de la red empresarial (LAN y WAN), señalando los factores que deben considerarse para la selección del medio de transmisión ideal y mencionando las medidas de seguridad necesarias que deben adoptarse con el objetivo de implantar un sistema confiable que permita el crecimiento de la organización y su competitividad en el mercado actual.

Objetivos

Objetivo General

Identificar los elementos clave, así como los principales factores que afectan la seguridad de un sistema de transmisión de datos, con el fin de proveer los mecanismos mínimos de seguridad que permitan mantener la integridad y confiabilidad de la información que fluye a través de la red empresarial.

Objetivos Particulares

- Definir los conceptos fundamentales relacionados con las telecomunicaciones que nos permitan entender las diversas técnicas existentes en el proceso de transmisión de información.
- Conocer las características básicas y las propiedades de los diferentes medios de transmisión utilizados para la interconexión de redes con el fin de tener un panorama más amplio de las posibilidades actuales.
- Describir el funcionamiento de las tecnologías LAN y WAN más importantes, utilizadas actualmente, para la implantación de la red empresarial.
- Puntualizar algunos conceptos básicos sobre seguridad y señalar los múltiples tipos de amenazas, vulnerabilidades y ataques que afectan la integridad y confidencialidad de la información.
- Mencionar los diferentes mecanismos de protección de la información al momento de transmitirla a través de la infraestructura de comunicaciones de la empresa y/o hacia Internet con el fin de conservar el valor de la información.
- Establecer las condiciones ideales para diseñar e implantar un sistema de comunicaciones de datos que cuente con los mecanismos de seguridad adecuados para asegurar la veracidad de la información transmitida.

Hipótesis

En las condiciones tecnológicas actuales es posible diseñar un sistema de comunicaciones funcional que cubra los requisitos mínimos de seguridad protegiendo la información generada en la organización que circula a través de la red interna y/o hacia Internet.

CAPÍTULO 1

Introducción a las Comunicaciones de Datos

1.1. Evolución Histórica de las Telecomunicaciones

La historia de las telecomunicaciones comenzó en 1832 cuando el artista e inventor Norteamericano Samuel Morse (1791 – 1872) tuvo la idea de un sistema de transmisión codificada utilizando puntos y guiones e inventó el ahora famoso código Morse. En 1837 se realizó la primera prueba y en 1840 fue patentado. "La primera conexión oficial tuvo lugar en 1844 y para 1851 aproximadamente 50 compañías de telégrafo estaban en operacion"[1]. Durante el resto de la década de los 1850's el sitema Morse fue adoptado internacionalmente.

En 1876, la oficina de patentes de los Estados Unidos publicó una patente a Alexander Graham Bell por su invención del teléfono y en 1877 se formó la compañía telefónica Bell. Un usuario debería tener un par de cables telefónicos conectados directamente al teléfono para poder recibir una llamada, además los teléfonos no contaban con timbres, por lo tanto los usuarios que deseaban establecer una comunicación deberían estar enlazados entre sí al mismo tiempo.

En 1878 la compañía Bell instaló la primera central telefónica con un operador, el cual podía comunicar a un usuario a diferentes sitios utilizando puentes de alambre para cerrar el circuito.

En 1885, se formó la American Telephone and Telegraph Company (AT&T) para operar y construir líneas de larga distancia para interconectar a las compañías telefónicas regionales.

En 1892 comenzó el switcheo automático con la introducción del primer disco de marcado en La Porte, Indiana. Este sistema trabajaba utilizando una serie de switches selectores electromecánicos, llamados "relays", para colocar automáticamente la llamada entrante en la línea de salida correcta. Las llamadas de disco tenían un tiempo deliberado de espera después de que los 8 dígitos eran marcados para darle tiempo al switch de establecer la conexión. El switch electromagnético fue reemplazado por el switch

[1] Ramos, Emilio y Schroeder, Al. 1994. Ed. Macmillan Publishing Company, "Concepts of Data Communications".

electrónico, con lo que se redujo el retardo usado por los relays y los teléfonos de botones comenzaron a ser usados para realizar la conexión.

En 1899 Guglielmo Marconi (1874 – 1937) realizó el primer enlace telegráfico utilizando ondas de radio entre Francia e Inglaterra, pero fue Lee de Forest (1873 – 1961) cuya invencion de la válvula de triodo abrió el camino para las comunicaciones de larga distancia y en 1927 tuvo lugar el primer enlace radio-telefonico transatlantico.

En 1913 se inventó el tubo de vacio (bulbo) y en 1941 se produjo la integración de las computadoras y las comunicaciones, con lo cual se aceleró el uso y desarrollo de nuevos sistemas, disminuyendo el costo de la comunicación e incrementando la calidad y la eficiencia.

En 1938 Alec Reeves describió el principio del código numérico de señales (Pulse Code Modulation, PCM) y en 1943 se desarrollaron los amplificadores sumergibles y repetidores facilitando la comunicación a través de largas distancias y entre clientes internacionales.

Este proceso evolutivo fue ampliamente acelerado por la invención del transistor en 1947 (por Bardeen, Brattain y Shockley de los laboratorios Bell), el cual, por su bajo poder de consumo y consecuente baja generación de calor vino a revolucionar los circuitos electrónicos, así como la industria de las telecomunicaciones ya que permitió el desarrollo de computadoras mas rápidas y pequeñas, las cuales tenian un menor costo y estaban al alcance de muchas compañías. Este hecho permitió que en 1956 se instalara el primer cable telefónico transoceánico con 15 repetidores sumergidos.

La tecnología de circuitos integrados propició el desarrollo de satélites expandiendo las oportunidades dentro del mundo de las comunicaciones de datos y "para 1962 el satélite artificial Telstar 1 fue puesto en servicio. En 1978 se realizó el primer enlace numérico (Transfix) y en 1979 se instaló en Francia la primera red mundial para la transmisión de datos en paquetes (X25) (Transpac)"[2].

Actualmente los servicios de telecomunicaciones son innumerables, entre los más populares se encuentran el fax, modems, internet y servicios de tarjeta de crédito.

1.2. Formas de Transmisión de la Información

La información pueden clasificarse en analógica y digital dependiendo de su naturaleza y la transformación que necesita para su procesamiento por los sistemas manejadores de datos.

[2] Servin, Claude. 1999. Ed. Springer. "Telecommunications: Tranmission and Network Arquitecture".

Adicionalmente la transmisión de información se agrupa en 3 grandes áreas de acuerdo a:

a) Como fluyen los datos a través de los dispositivos.
b) El tipo de conexión física.
c) El tipo de sincronización usado para transmitir datos.

Los datos pueden fluir en modo simplex, half-duplex o full-duplex; la conexión física puede ser paralela o serial y la sincronización puede ser síncrona o asíncrona.

1.2.1. Clasificación de la Información

a) Analógica o Datos Continuos. Es el resultado de una variación continua de fenómenos físicos tales como la temperatura, voz, imagen, etc. "Un sensor las convierte en una corriente eléctrica proporcional a la amplitud del fenómeno físico analizado, lo cual produce una señal analógica, debido a que esta señal varía en forma análoga al fenómeno físico original"[3]. Una señal analógica puede tener un número infinito de valores en un intervalo de tiempo dado.

b) Digital o Datos Discretos. "Es la información resultante de un conjunto de elementos que son independientes unos de otros"[4], por ejemplo, un texto es una asociación de palabras, las cuales están compuestas de letras (símbolos elementales). Para manejar este tipo de información, el equipo debe sustituir un número binario único para cada elemento de información. Esta operación se denomina información codificada para información discreta y digitalización de la información para información analógica.

1.2.2. Modos de Transmisión de Acuerdo al Flujo de Datos

a) Modo Simplex o Unidireccional. El intercambio de datos se realiza en una sola dirección sobre el medio físico y cada dispositivo tiene solamente una función, como transmisor o receptor, ejemplos de este tipo de comunicación son las transmisiones de radio y televisión (Figura 1.1).

b) Modo Half-Duplex. La transmisión es permitida en cualquier dirección sobre el circuito, pero solamente en una dirección a la vez, este tipo de transmisión es ampliamente utilizada en aplicaciones de procesamiento de datos. Si dos dispositivos se comunican en modo half-duplex y ambos transmiten al mismo tiempo, entonces los datos enviados no son recibidos o simplemente se convierten en basura en las líneas (Figura 1.1).

c) Modo Full-Duplex o Bidireccional. Permite la transmisión simultánea de datos en ambas direcciones, la mayoría de las computadoras están configuradas para trabajar en este modo; este tipo de transmisión requiere mayor control de hardware y software en

[3] Ramos, Emilio y Schroeder, Al. 1994. Ed. Macmillan Publishing Company, "Concepts of Data Communications".
[4] Idem

ambos sentidos. Aunque este es el modo de transmisión mas complejo, es también el más eficiente (Figura 1.1).

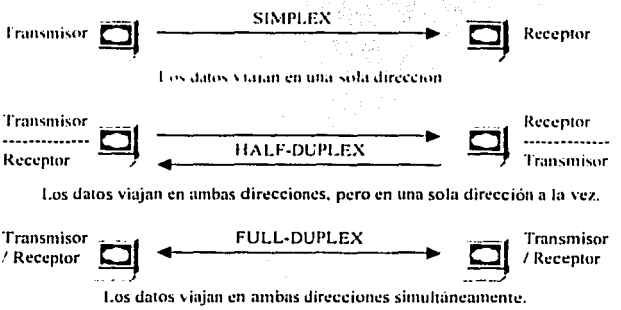


Figura 1.1: Clasificación de acuerdo al Flujo de Datos.

1.2.3. Modos de Transmisión de Acuerdo a la Conexión Física

La transmisión de datos puede ser clasificada en base a la cantidad de bits transmitidos con cada pulso del reloj y se divide en comunicación paralela o simultánea y comunicación serial o secuencial. Los puertos de entrada/salida del dispositivo de procesamiento de datos pueden transmitir los datos bit por bit o enviar un byte completo en una sola operación en paralelo empleando 8 líneas, una para cada bit.

a) Transmisión en Paralelo. Se caracteriza por la transmisión simultánea de todos los bits de la misma palabra, lo que requiere tantos conductores como bits a transmitir. El beneficio de la transmisión en paralelo es la simplicidad, un byte es colocado en el puerto de salida del dispositivo y un solo pulso del reloj de la computadora transfiere los datos al dispositivo receptor; sin embargo, debido al número de cables involucrados y a la pérdida de la señal sobre distancias relativamente cortas es impráctico usar puertos paralelos para comunicaciones sobre largas distancias. El ejemplo más común de este tipo de transmisión es el enlace entre computadora e impresora (Figura 1.2).

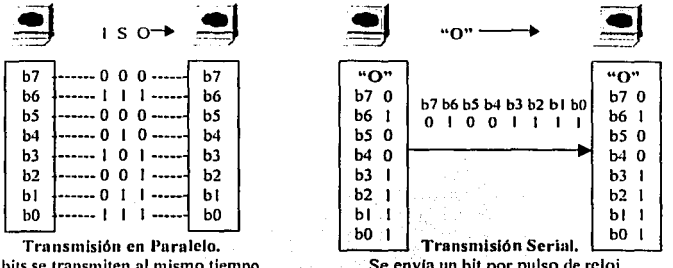


Figura 1.2: Clasificación de acuerdo a la Conexión Física.

b) Transmisión Serial. Todos los bits de una palabra o de un mensaje son transmitidos secuencialmente a través de la misma línea para proveer la comunicación entre dispositivos. "En las computadoras, los datos (bits) son tratados en paralelo, por lo que se requiere una interfase de conversión de bits paralelo → serial durante la transmisión y de serial → paralelo al recibir los datos; las líneas telefónicas estándar también pueden ser usadas para transmitir datos en forma serial"[5] Para transmisiones de datos, la transmisión serial necesita solo dos conductores, de esta manera el costo es menor y puede utilizarse para transmisiones sobre distancias considerables; aunque la transmisión de datos en este modo es más lenta que la transmisión en paralelo, hoy en día es ampliamente utilizada para la transmisión de datos (Figura 1.2).

1.2.4. Modos de Transmisión de Acuerdo a la Sincronización

Sincronización se refiere a como sabe el dispositivo receptor que ha recibido un grupo de bits, los cuales forman un caracter válido; existen dos variantes: "si varios caracteres del mensaje que será transmitido son enviados en forma irregular se denomina transmisión asíncrona; si todos los caracteres son agrupados en bloques transmitidos irregularmente, donde no hay un enlace cronológico entre los bloques, pero si existe entre todos los bits del mismo bloque, se denomina transmisión síncrona"[6].

En transmisiones seriales, los bits de un mismo caracter son espaciados en forma regular, pero el intervalo que separa dos caracteres puede ser variable, a esto se le denomina transmisión asíncrona.

a) Comunicación Asíncrona. Se caracteriza por el uso de un bit de start precediendo a cada caracter transmitido, además existen uno o más bits de stop al final de cada caracter. El bit (o bits de stop) corresponde a un tiempo mínimo de descanso del sistema entre la transmisión o recepción de dos caracteres sucesivos. Los datos se envían en ráfagas irregulares y no en flujos constantes (Figura 1.3).

Los bits de start y stop forman lo que se llama un frame de caracter; cada caracter debe ser colocado en un frame. El receptor cuenta el bit de start y el número apropiado de bits de datos, si el final del frame no es coherente, entonces se produce un error en el frame y se recibe un caracter inválido; cuando esto ocurre, los sistemas inteligentes solicitan la retransmisión del último grupo de bits.

La transmisión asíncrona es relativamente simple y barata para su implementación; es ampliamente usada en microcomputadoras y dispositivos comerciales de comunicaciones. Sin embargo tiene una baja eficiencia de transmisión debido a que al menos dos bits extras deben agregarse a cada caracter transmitido. Tradicionalmente, "las

[5] Idem
[6] Collin, Serge. 1990. Ed. Prentice-Hall International. "Computer, Interfaces and Communications".

comunicaciones asíncronas tienen una velocidad baja , desde 3,000 a 19,200 baudios, pero en algunos casos la velocidad de transmisión puede ser mayor"[7].

b) Comunicación Síncrona. Al contrario de la transmisión asíncrona que utiliza bits de start y stop que agregan overhead al flujo de bits, en la comunicación serial síncrona no se utilizan bits de start y stop. Todos los bits del mismo mensaje son espaciados regularmente; los caracteres de datos son agrupados en grandes grupos llamados bloques. La transmisión de diferentes bloques (o frames) puede ser irregular: como en la transmisión asíncrona, y el comienzo y el final del objeto que será transmitido, en este caso un bloque, debe estar delimitado. Los bloques son delimitados por caracteres especiales (banderas de start y stop) reconocidos por el protocolo utilizado; la bandera de stop de un bloque puede servir como la bandera de start del siguiente. Cuando el receptor detecta uno de estos caracteres especiales, sabe que el siguiente bit es el comienzo de un caracter manteniendo así la sincronización (Figura 1.3).

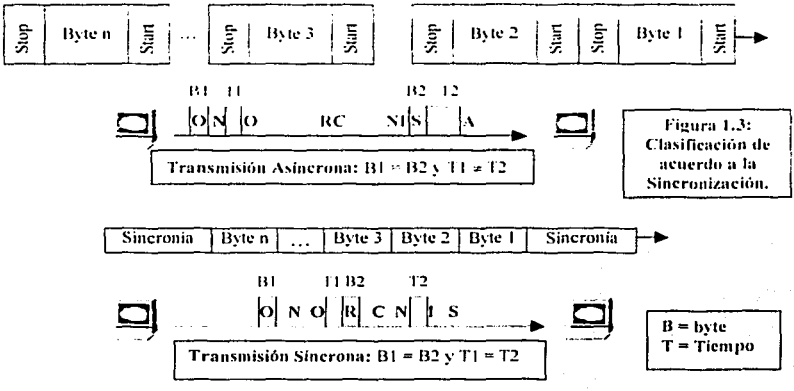


Figura 1.3: Clasificación de acuerdo a la Sincronización.

1.3. Fundamentos de Multiplexaje

El multiplexaje es un proceso en el que varios canales de datos se combinan en un solo canal físico en el origen, las transmisiones ocurren en el mismo medio pero no necesariamente al mismo tiempo; este proceso se puede implementar en cualquier capa del modelo OSI (Open Systems Interconnection). El demultiplexaje es el proceso de separar en el destino los canales de datos multiplexados.

[7] Idem

Un multiplexor es un dispositivo de la capa física que combina múltiples ráfagas de datos en uno o más canales de salida en el origen, dichos dispositivos demultiplexan los canales en varias ráfagas de datos en el extremo remoto, minimizando el uso de ancho de banda del medio físico y permitiendo que éste sea compartido por varias fuentes de tráfico.

1.3.1. Importancia del Multiplexaje

El multiplexaje permite hacer un uso eficiente de las líneas de telecomunicaciones de alta velocidad, de tal forma que varias fuentes de transmisión compartan una capacidad de transmisión superior.

Es importante para las comunicaciones intercontinentales, en las cuales se combinan muchas conversaciones telefónicas y luego se transmiten por un satélite de comunicaciones o cable submarino.

Los enlaces de las redes de larga distancia (líneas de fibra, cable coaxial o de microondas de alta capacidad), transportan simultáneamente varias transmisiones de voz y de datos mediante el uso de las técnicas de multiplexaje.

1.3.2. Técnicas de Multiplexaje

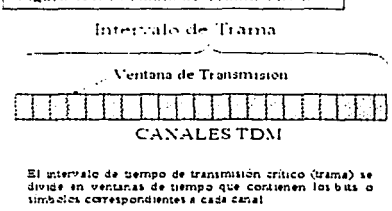
a) TDM (Time Division Multiplexing). "Asigna ancho de banda a la información de cada canal de datos con base en ranuras de tiempo preasignadas, sin tomar en cuenta si hay datos para enviar o no"[8] (Figura 1.4). Sus características son:

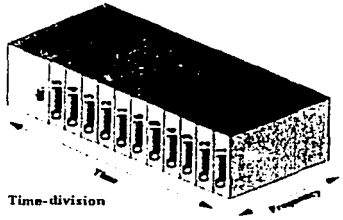
- Se lleva a cabo cuando la velocidad de transmisión alcanzable por el medio es mayor que la velocidad de las señales a transmitir.
- Transporte de varias señales digitales (o analógicas) a través de una ruta única de transmisión mediante la mezcla temporal de las partes de cada una de ellas.
- La transmisión es generalmente síncrona.
- Los datos se transmiten mediante formato de tramas.
- Independientemente de como se lleve a cabo el multiplexaje, se pueden incorporar varias formas de estructuras de bits, cada una de las cuales representa la unidad mínima de tiempo en la que todas las señales multiplexadas se transmiten al menos una vez.
- En la trama se deben agregar palabras de bits para la estructura y la sincronía para permitir que el sistema receptor se sincronice en el tiempo con el inicio de cada estructura, con cada espacio de ella y con cada bit contenido en estos espacios. Estos bits pueden denominarse en forma colectiva bit(s) de control.
- La técnica TDM síncrona obedece su nombre a las ranuras temporales preasignadas y fijadas a las diferentes fuentes.
- Dedica una ranura de tiempo a cada estación.
- La TDM es eficiente para un número de estaciones pequeñas y tráfico continuo.

[8] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".

- Las técnicas TDM por lo general son preferidas a las técnicas FDM (Frecuency Division Multiplexing) ya que la transmisión de datos libres de error e información de voz es facil.

Figura 1.4: Formato de Trama TDM.

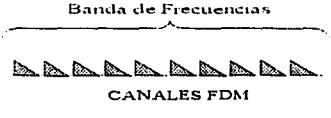


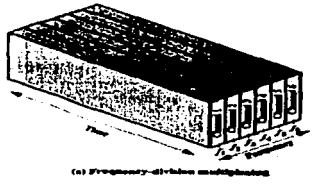


b) FDM (Frecuency Division Multiplexing). "Asigna ancho de banda a la información de cada canal de datos con base en la frecuencia de la señal del tráfico"[9] (Figura 1.5). Sus carácteristicas son:

- Es posible utilizar el FDM cuando el ancho de banda útil del medio de transmisión supera el ancho de banda requerido por las señales a transmitir.
- Hay simultaneidad en la transmisión de señales porque cada una de ellas se modula con una frecuencia portadora diferente, tal que estas frecuencias están suficientemente separadas para que no se solapen significativamente las señales.
- La señal compuesta transmitida a través del medio es analógica.
- Las señales de entrada siempre deben ser moduladas, para trasladarlas a la banda de frecuencia apropiada.
- Si la señal de entrada es digital, se debe pasar a través de un modem para convertirla en analógica y modularla posteriormente.

Figura 1.5: Formato de Trama





[9] Idem

c) STDM (Statistical Time Division Multiplexing). "Asigna ancho de banda de manera dinámica a cualquier canal de datos que tenga información para transmitir"[10] (Figura 1.6).

Usualmente las terminales no siempre están transmitiendo información, por lo que existen periodos de tiempo (tiempo muerto) en los cuales los dispositivos no están siendo utilizados. Los multiplexores estadísticos son dispositivos inteligentes capaces de identificar que terminales no están siendo utilizadas y que terminales necesitan transmitir, los cuales asignan el tiempo necesario para la transmisión solamente cuando se requiere. Esto significa que el tiempo para la transmisión se provee solamente cuando una terminal necesita transmitir datos.

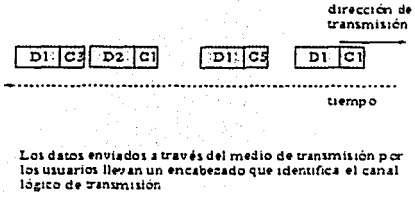


Figura 1.6: Transmisión en STDM.

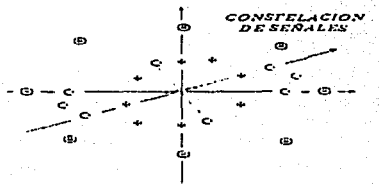
d) CDMA (Code Division Multiplexing). (Figura 1.7). Algunas catacterísticas de este método son:

- No hay restricciones de tiempo o de ancho de banda.
- Cada transmisor de estación terrena puede transmitir cada vez que lo desea y puede utilizar cualquier ancho de banda o todos los anchos de banda asignados a un sistema o canal de satélite en particular.
- El CDMA también es conocido como acceso múltiple del espectro disperso debido a que no hay limitaciones en el ancho de banda.
- Las transmisiones son separadas por medio de técnicas de cifrado. Las transmisiones de cada estación terrena se codifican con una única palabra binaria llamada código de chip.
- Para recibir la transmisión de una estación terrena en particular, la estación receptora tiene que saber el código de chip para esa estación.
- La ventaja más importante es su inmunidad a la interferencia que hace que el CDMA sea ideal para las aplicaciones militares.
- Con CDMA, todas las estaciones terrenas dentro del sistema pueden transmitir a la misma frecuencia y al mismo tiempo.
- Una de las ventajas de CDMA es que todo el ancho de banda de un canal o sistema satelital puede utilizarse para cada transmisión de toda estación terrena.

[10] Ídem

- El salto de frecuencia es una forma de CDMA en donde un código digital se utiliza para cambiar continuamente la frecuencia de la portadora.

Figura 1.7: Flujo de Señales en CDMA.

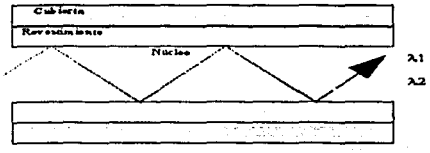


El código de señales se divide entre los distintos canales

e) WDM (Wavelength Division Multiplexing). "Método para multiplicar la capacidad de una fibra óptica mediante la operación de más de una longitud de onda. Diferentes frecuencias son seleccionadas mediante el uso de filtros sensibles a la luz, los cuales combinan frecuencias lumínicas, las envían y separan en el extremo receptor"[11] (Figura 1.8).

Todo el potencial de la fibra se utiliza plenamente cuando se transmiten varios haces de luz a diferentes frecuencias en la misma fibra. En WDW, el haz de luz está constituido por una multitud de colores o longitudes de onda, cada uno de los cuales porta un canal diferente de datos. "En 1997 se alcanzó un hito cuando en los laboratorios Bell se demostró la viabilidad de un sistema WDM con 100 haces cada uno operando a 10 Gbps, proporcionando una velocidad de transmisión total de un trillón de bits por segundo (1 Terabit por segundo Tbps). Ya están disponibles en le mercado sistemas con 80 canales a 10 Gbps cada uno"[12].

Figura 1.8: Longitudes de Onda en WDM.



Cada longitud de onda de luz constituye un canal diferente

[11] Ramos, Emilio y Schroeder, Al. 1994, Ed. Macmillan Publishing Company, "Concepts of Data Communications".
[12] Idem

1.4. El Modelo de Referencia OSI (Open Systems Interconnection)

El modelo de referencia OSI describe como se transfiere la información desde una aplicación de software en una computadora a través del medio de transmisión hasta una aplicación de software en otra computadora; fue desarrollado por la ISO (International Organization for Standardization) en 1984 y es considerado como el modelo principal de arquitectura para la comunicación entre computadoras. OSI divide las funciones implicadas en la transferencia de información entre computadoras en 7 grupos de tareas más pequeñas y fáciles de manejar. Cada capa es razonablemente individual, por lo que las tareas asignadas a cada capa se pueden implementar de manera independiente, lo que permite que las soluciones ofrecidas por una capa se puedan actualizar sin afectar a las demás.

Tabla 1.1: Principios utilizados en la definición de las capas OSI (ISO 7498)

1. No crear demasiadas capas de forma que la descripción e integración de las capas sea más difícil de lo estrictamente necesario.
2. Definir separaciones entre capas tal que la descripción de servicios sea pequeña y el número de interacciones entre capas sea mínimo.
3. Definir capas separadas para funciones que sean claramente diferentes, en lo que respecta al servicio ofrecido así como a la tecnología implicada.
4. Definir funciones similares en la misma capa.
5. Seleccionar los límites o separación entre capas de acuerdo con lo que la experiencia previa aconseje.
6. Definir las capas tal que las funciones se puedan localizar fácilmente de forma que la capa se pueda rediseñar completamente y tal que sus protocolos se puedan modificar para adaptarse a las innovaciones en la arquitectura, la tecnología hardware o en el software sin necesidad de cambiar los servicios que se usan o proporcionan en las capas adyacentes.
7. Definir una separación entre capas, ahí donde pueda ser útil tener la interfaz correspondiente normalizada.
8. Crear una capa donde exista la necesidad de un nivel diferente de abstracción en el procesamiento de los datos (por ejemplo, morfológico, sintáctico, semántico).
9. Permitir modificaciones de funciones o protocolos dentro de una capa siempre que no afecten a otras capas.
10. Crear para cada capa límites o separaciones sólo con su capa superior o inferior.

Principios similares han sido aplicados para la creación de subcapas.

11. Crear subgrupos y organizaciones adicionales de funciones en subcapas dentro de una capa sólo en los casos donde se necesiten servicios distintos de comunicación.
12. Crear, donde sea necesario, dos o más subcapas con una funcionalidad común y por lo tanto mínima para permitir la operación de la interfaz con capas adyacentes.
13. Permitir la no utilización de todas las subcapas.

1.4.1. División de las Capas del Modelo OSI

Las 7 capas del modelo OSI se pueden dividir en dos categorías: capas superiores y capas inferiores (Figura 1.9).

"Las capas superiores del modelo OSI tienen que ver con la aplicación y en general están implementadas sólo en software. la capa superior, la de aplicación, es la más cercana al usuario final"[13]. El término capa superior se usa a veces para referirse a cualquier capa que este sobre otra capa en el modelo OSI.

"Las capas inferiores del modelo OSI manejan lo concerniente a la transferencia de datos: las capas física y de enlace de datos se encuentran implementadas en hardware y software. En general, las demás capas inferiores están implementadas únicamente en software"[14].

Figura 1.9:
Subcapas del Modelo OSI.

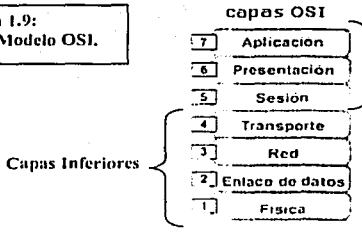


Tabla 1.2: Justificación de las capas OSI (ISO 7498)

1. Es esencial que la arquitectura permita la utilización de una realización realista de medios físicos para la interconexión con diferentes procedimientos de control (por ejemplo V.24, V.25, etc.). La aplicación de los principios 3, 5 y 8 (Tabla 1.1) nos conduce a la identificación de la **Capa Física** como la capa más baja de la arquitectura.
2. Algunos medios de comunicación físicos (por ejemplo la línea telefónica) requieren técnicas específicas para usarlos al transmitir datos entre sistemas a pesar de sufrir una tasa de error elevada (inaceptable para la gran mayoría de las aplicaciones). Estas técnicas específicas se utilizan en procedimientos de control del enlace de datos que han sido estudiados y normalizados durante varios años. También se debe reconocer que los nuevos medios de comunicación (por ejemplo la fibra óptica) requieren diferentes procedimientos de control del enlace de datos. La aplicación de los principios 3, 5 y 8 nos conduce a la identificación de la **Capa de Enlace de Datos** situada encima de la capa física en la arquitectura.

[13] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".
[14] Idem

3. En la arquitectura OSI, algunos sistemas serán (actuarán como) el destino final de los datos. Algunos sistemas abiertos podrían actuar solamente como nodos intermedios (reenviando los datos a otros sistemas). La aplicación de los principios 3, 5 y 7 conduce a la identificación de la **Capa de Red** encima de la capa de enlace de datos. Así, la capa de Red proporcionará un camino de conexión (conexión de red) entre un par de entidades de transporte incluyendo el caso en el que estén involucrados nodos intermedios.

4. El control del transporte de los datos desde el sistema final origen al sistema final destino (que no se lleva a cabo en nodos intermedios) es la función que realiza el servicio de transporte. Así, la capa superior situada justo encima de la capa de red es la **Capa de Transporte**. Esta capa libera a las entidades de capas superiores de cualquier preocupación sobre el transporte de datos entre ellas.

5. Existe una necesidad de organizar y sincronizar el diálogo, y controlar el intercambio de datos. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **Capa de Sesión** situada sobre la capa de transporte.

6. El conjunto restante de funciones de interés general son aquellas relacionadas con la representación y la manipulación de datos estructurados para el beneficio de los programas de aplicación. La aplicación de los principios 3 y 4 nos conduce a la identificación de la **Capa de Presentación** situada sobre la capa de sesión.

7. Finalmente, están las aplicaciones que llevan a cabo el procesamiento de la información. La **Capa de Aplicación**, que es la más alta de la arquitectura aborda parcialmente este procesamiento junto con los protocolos involucrados.

1.4.2. Características de las Capas del Modelo OSI

A continuación se describen las características principales de las capas del modelo OSI, así como sus principales funciones (Figura 1.10).

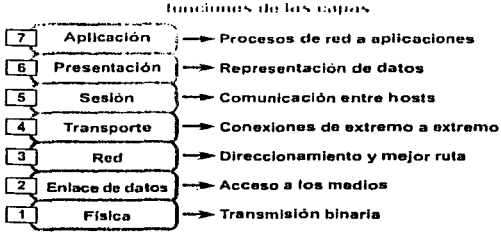


Figura 1.10: Funciones de las Capas del Modelo OSI.

a) Capa Física

Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de redes de comunicaciones; las especificaciones de la capa física definen características como niveles de voltaje, temporización de cambios de voltaje, velocidades de transferencia de información, distancias máximas de transmisión y conectores físicos.

b) Capa de Enlace de Datos

"Proporciona el tráfico confiable de datos a través del enlace de red, diferentes especificaciones en esta capa definen diferentes características de red y protocolo, incluyendo el direccionamiento físico, la topología de red, la especificación de error, la secuencia de tramas y el control de flujo"[15]. El direccionamiento físico define como se nombran los dispositivos en la capa de enlace de datos; la topología de red consiste en especificaciones de la capa de enlace de datos, que con frecuencia definen la forma en que se conectarán físicamente los dispositivos (en forma de bus o anillo); la notificación de error alerta a los protocolos de las capas superiores cuando se presenta un error en la transmisión y la secuencia de tramas de datos reordena las que se han transmitido fuera de secuencia; el control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con mas tráfico del que pueda manejar simultáneamente.

El IEEE (Institute of Electrical and Electronics Engineers) ha subdividido la capa de enlace en dos subcapas: LLC (Logical Link Control) y MAC (Medium Access Control).

La subcapa LLC de la capa de enlace de datos administra las comunicaciones entre los dispositivos unidos por un enlace individual de red; está definida en la especificación IEEE 802.2 y soporta los servicios orientados y no orientados a la conexión utilizados por los protocolos de las capas superiores. El IEEE 802.2 define varios campos en las tramas de la capa de enlace de datos que permiten que varios protocolos de las capas superiores compartan un solo enlace físico de datos.

La subcapa MAC de la capa de enlace de datos administra el protocolo de acceso al medio de transmisión físico de la red; la especificación IEEE MAC define las direcciones MAC, las cuales permiten a múltiples dispositivos identificarse de manera única entre sí en la capa de enlace de datos.

c) Capa de Red

Proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos combinarse en una red; esto se logra a través del direccionamiento lógico de los dispositivos. Algunos protocolos comunes de ruteo son BGP (Border Gateway Protocol),

[15] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

un protocolo de ruteo entre dominios de Internet, el protocolo de compuerta interior OSPF (Open Shortest Path First), basado en estado de enlaces y desarrollado para utilizarse en redes TCP/IP (Transmission Control Protocol / Internet Protocol) y el protocolo RIP (Routing Information Protocol), un protocolo de ruteo de Internet que utiliza el conteo de saltos como su métrica.

d) Capa de Transporte

Implanta servicios confiables de datos entre redes que son transparentes a las capas superiores. Entre sus funciones más importantes están el control de flujo, el multiplexaje, la administración de circuitos virtuales y la verificación y recuperación de errores.

El control de flujo administra la transmisión de datos entre dispositivos para que el transmisor no envíe más datos de los que pueda procesar el dispositivo receptor; el multiplexaje permite que los datos de diferentes aplicaciones sean transmitidos en un enlace físico único. Esta capa establece, mantiene y termina los circuitos virtuales. La verificación de errores implica la creación de varios mecanismos para detectar los errores en la transmisión, en tanto que la recuperación de errores implica realizar una acción, como solicitar la retransmisión de los datos para resolver cualquier error que pueda ocurrir.

e) Capa de Sesión

Establece, administra y finaliza las sesiones de comunicación entre las entidades de la capa de presentación; las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas entre diferentes dispositivos de red. Estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión.

f) Capa de Presentación

Brinda una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación, dichas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea legible por la capa de aplicación de otro sistema. Algunos ejemplos de esquemas de codificación y conversión de esta capa incluyen formatos de representación de datos comunes y esquemas de cifrado de datos comunes.

Los formatos de presentación de datos comunes o el uso de formatos estándar de video, sonido e imagen, permiten el intercambio de datos de aplicación entre diferentes tipos de sistemas de computadoras; los esquemas de conversión se utilizan para intercambiar información entre sistemas utilizando diferentes representaciones de texto y datos, como EBCDIC (Extended Binary-Coded Decimal Interchange Code) y ASCII (American Standard Code for Information Interchange). Los esquemas estándar de compresión de datos permiten que los datos que se comprimen en el dispositivo fuente se puedan descomprimir adecuadamente en el destino; los esquemas estándar de cifrado de

datos permiten que los datos cifrados en el dispositivo fuente sean descifrados de manera adecuada en el destino.

g) Capa de Aplicación

Esta es la capa del modelo OSI más cercana al usuario final, por lo que interactúa con el usuario y con la aplicación de software de manera directa. Las funciones de la capa de aplicación incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de los recursos y la sincronización de la comunicación.

Al identificar socios de comunicación la capa de aplicación determina su identidad y disponibilidad para una aplicación que debe transmitir datos; cuando se está determinando la disponibilidad de los recursos, la capa de aplicación debe decidir si hay suficientes recursos en la red para la comunicación que se está solicitando. Al sincronizar la comunicación, toda comunicación entre aplicaciones requiere cooperación, y ésta es administrada por la capa de aplicación.

CAPÍTULO 2

Medios de Transmisión de Datos

Todos los equipos de comunicaciones de datos necesitan algún tipo de medio de transmisión para que ésta pueda llevarse a cabo; aunque muchos administradores toman la decisión de que tipo de medio de transmisión utilizar en base al volumen de datos y la velocidad de transmisión que soportan, existen otros factores que afectan el éxito de la implantación de un sistema de transmisión de datos. La selección del medio adecuado es el elemento clave para una operación exitosa del sistema.

En los sistemas de transmisión de datos, el medio de transmisión es el camino físico entre el transmisor y el receptor; los medios de transmisión se clasifican en guiados y no guiados, en ambos casos la comunicación se lleva a cabo con ondas electromagnéticas. En los medios guiados las ondas se confinan en un medio sólido como el par trenzado de cobre, el cable coaxial de cobre o la fibra óptica. La atmósfera o el espacio exterior son ejemplos de medios no guiados que proporcionan un medio de transmisión de las señales pero sin confinarlas, esto se denomina transmisión inalámbrica.

Las características y la calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio en sí mismo es lo más importante en la determinación de las limitaciones de transmisión.

"En medios no guiados, el ancho de banda de la señal transmitida por la entena es más importante que el propio medio a la hora de determinar las características de la transmisión; una propiedad fundamental de este tipo de señales es la directividad, puesto que generalmente a frecuencias bajas las señales son omnidireccionales, es decir, la señal desde la antena se emite y propaga en todas direcciones, mientras que a frecuencias más altas es posible concentrar la señal en un haz direccional"[1].

En el diseño de sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grande posible. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión:

- Ancho de banda. Si los demás factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión se puede incrementar.

[1] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

- Dificultades en la transmisión. Las dificultades como la atenuación limitan la distancia; en los medios guiados el par trenzado sufre mayores adversidades que el cable coaxial, que a su vez es más vulnerable que la fibra óptica.
- Interferencias. Las interferencias resultantes de la presencia de señales en bandas de frecuencias próximas pueden distorsionar o destruir completamente la señal; las interferencias son especialmente relevantes en los medios no guiados, pero son a la vez un problema a considerar en los medios guiados.
- Número de receptores. Un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido mediante el uso de múltiples conectores; cada conector puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirán.

2.1. Medios de Transmisión Guiados

Los medios de transmisión guiados trabajan conectando al transmisor directamente al medio físico, el transmisor puede ser una microcomputadora, una terminal o un dispositivo periférico; la señal viaja a través del cable y en el otro extremo el receptor está igualmente directamente conectado al medio.

En los medios de transmisión guiados, la capacidad de transmisión, en términos de su velocidad o ancho de banda, depende drásticamente de la distancia y de si el medio se usa para un enlace punto a punto o para un enlace multipunto.

Los tres medios guiados más utilizados para la transmisión de datos son el par trenzado, el cable coaxial y la fibra óptica.

2.1.1. Par Trenzado

El par trenzado es el medio guiado más económico y a la vez el más usado.

a) Descripción Física

"El par trenzado consiste en dos pares de cobre embutidos en un aislante entrelazados en forma de espiral; cada par de cables constituye sólo un enlace de comunicación"[2] (Figura 2.1). Normalmente se utilizan haces en los que se encapsulan varios pares en una envoltura protectora. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura; para este fin, los pares adyacentes dentro de una misma envoltura protectora se trenzan con pasos de torsión diferentes, para enlaces de larga distancia la longitud del trenzado varía entre 5 y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0.4 y 0.9 mm.

[2] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Primer Año".

Figura 2.1:
Par Trenzado.

Longitud del Trenzado

- Aislado independientemente.
- Trenzado conjuntamente.
- A veces embutido en un cable.
- Normalmente se instala en los edificios en construcción.

b) Aplicaciones

Se usa tanto para señales analógicas como para señales digitales; es el medio más usado en las redes de telefonía, al igual que en las redes de comunicación dentro de edificios.

En señalización digital los pares trenzados se utilizan para las comunicaciones al conmutador digital o PBX (Private Branch Exchange) digital, con velocidades de 64 kbps. El par trenzado también se utiliza en redes de área local dentro de edificios para la conexión de computadoras personales, su velocidad típica es de 10 Mbps, no obstante, actualmente se han desarrollado redes de área local con velocidades entre 100 Mbps y 1 Gbps mediante pares trenzados, aunque estas configuraciones están limitadas por el número de posibles dispositivos conectados, así como la extensión geográfica de la red. Para aplicaciones de larga distancia el par trenzado se puede utilizar a velocidades de 4 Mpbs e incluso mayores.

El par trenzado es mucho menos costoso que cualquier otro medio de transmisión guiado y a la vez es más sencillo de manejar. Comparado con el cable coaxial y la fibra óptica está más limitado en términos de velocidad de transmisión y de distancia máxima.

c) Características de Transmisión

"Para transmitir señales analógicas los cables de pares necesitan amplificadores cada 5 o 6 km; mientras que para la transmisión digital se requieren repetidores cada 2 o 3 km"[3].

Comparado con los demás medios guiados, el para trenzado permite menores distancias, menor ancho de banda y menor velocidad de transmisión; además existe una fuerte dependencia de la atenuación con la frecuencia. Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido debido a su fácil acoplamiento con campos electromagnéticos externos. Por ejemplo un cable conductor situado en paralelo con una línea de potencia que conduzca corriente alterna, se verá negativamente afectado por ésta; el ruido impulsivo también afecta los pares trenzados. Para reducir estos efectos negativos se puede blindar el cable con una malla metálica para reducir las interferencias externas; el trenzado en los cables reduce las interferencias de baja frecuencia y el uso de distintos pasos de torsión entre pares adyacentes reduce la diafonía.

[3] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

d) Pares Trenzados con Blindaje y sin Blindaje

Hay dos variantes de pares trenzados: con blindaje y sin blindaje. El par trenzado sin blindaje (UTP, Unshielded Twisted Pair) es el medio más habitual en telefonía. No obstante, actualmente es muy común su uso en el cableado de edificios para la transmisión de datos, ya que es el medio de transmisión menos caro, además de ser fácil de instalar y manipular.

El par trenzado sin blindaje puede verse afectado por interferencias electromagnéticas externas, incluyendo interferencias con pares cercanos y fuentes de ruido. Una manera de mejorar sus características de transmisión es embutiéndolo dentro de una malla metálica, reduciendo así las interferencias. El par trenzado con blindaje (STP, Shielded Twisted Pair) (Figura 2.2) proporciona mejores resultados a velocidades de transmisión bajas, sin embargo es más costoso y difícil de manipular que el UTP.

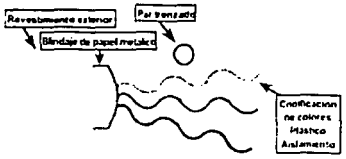


Figura 2.2: Cable STP.

- Velocidad y rendimiento 10 a 100 Mbps.
- Moderadamente caro.
- Longitud máxima del cable 100 m.

e) UTP (Unshielded Twisted Pair) Categoría 3 y Categoría 5

En 1991, la EIA (Electronic Industries Association) publicó el estándar EIA-568 denominado "Commercial Building Telecommunications Cabling Standard", que define el uso de pares trenzados sin blindaje de calidad telefónica y de pares con blindaje como medios para aplicaciones de transmisión de datos en edificios. Debido a la necesidad de mayores velocidades de transmisión, en 1995 se propuso la norma EIA-568-A, la cual incorpora los avances más recientes tanto en el diseño de cables y conectores así como en métodos de prueba; en esta especificación se consideran tanto pares de cables con blindaje a 150 Ohmios como pares sin blindaje de 100 Ohmios.

En el estándar EIA-586-A se consideran tres tipos de cables UTP:

- Tipo 3. Consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 16 MHz.
- Tipo 4. Consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 20 MHz.
- Tipo 5. Consiste en cables y su hardware asociado, diseñados para frecuencias de hasta 100 MHz (Figura 2.3).

Los tipos 3 y 5 son los más utilizados en los entornos LAN (Local Area Network); el tipo 3 corresponde a los cables de calidad telefónica que existen en la mayoría de los edificios. Con un diseño apropiado y a distancias limitadas, con cables tipo 3 se pueden

conseguir velocidades de hasta 16 Mbps. El cable tipo 5 (data grade) tiene mejores características para la transmisión de datos y es ampliamente utilizado en los edificios nuevos: con un diseño apropiado y a distancias limitadas, con cable tipo 5 se pueden alcanzar 100 Mbps.

"La diferencia esencial entre los cables tipo 3 y tipo 5 está en el número de trenzas por unidad de distancia: la longitud de la trenza en el tipo 5 es del orden de 0.6 a 0.85 cm, mientras que le tipo 3 tiene una trenza de 7.5 a 10 cm"[4]. El trenzado del tipo 5 es más caro y proporciona prestaciones superiores al del tipo 3.

El primer parámetro para establecer una comparación entre estos tipos de UTP y el STP es la atenuación, ya que la energía de la señal decrece con la distancia recorrida en el medio de trasmisión. En medios guiados la atenuación obedece a una ley logarítmica, por lo tanto se expresa como un número constante de decibelios por unidad de longitud (Tabla 2.1).

Tabla 2.1: Comparación de pares trenzados blindados y sin blindar.

	Atenuación (dB por 100 m)			Diafonía en el extremo final		
Frecuencia (MHz)	UTP Categoría 3	UTP Categoría 5	STP 150 Ohmios	UTP Categoría 3	UTP Categoría 5	STP 150 Ohmios
1	2.6	2.0	1.1	41	62	58
4	2.5	4.1	2.2	32	53	58
16	13.1	8.2	4.4	23	44	50.4
25	-	10.4	6.2	-	41	47.5
100	-	22.0	12.3	-	32	38.5
300	-	-	21.4	-	-	31.3

"La diafonía que sufren los sistemas basados en pares trenzados es debida a la inducción que provoca un conductor en otro cercano; por conductor debe entenderse tanto los pares que forman el cable, como los pines (patitas metálicas) del conector. Este tipo de diafonía se denomina cercana al extremo porque la señal transmitida en el enlace se acopla en un conductor cercano e induce una señal en sentido contrario (la energía transmitida es capturada por un par de recepción)"[5].

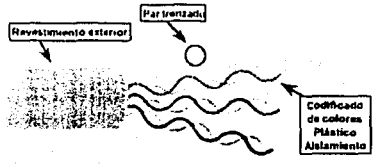


Figura 2.3: Cable UTP.

- Velocidad y rendimiento 10 a 100 Mbps.
- Precio económico.
- Longitud máxima del cable 100 m.

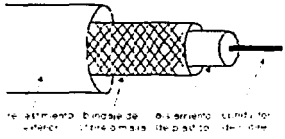
[4] Idem
[5] Idem

2.1.2. Cable Coaxial

a) Descripción Física

El cable coaxial, al igual que el par trenzado, tiene dos conductores, pero está construido de forma diferente para que pueda operar sobre un rango mayor de frecuencias. "Consiste en un conductor cilíndrico externo que rodea a un cable conductor; el conductor interior se mantiene a lo largo del eje axial mediante una serie de anillos aislantes regularmente espaciados o bien mediante un material sólido dieléctrico; el conductor exterior se protege con una cubierta o funda protectora. El cable coaxial tiene un diametro aproximado entre 1 y 2.5 cm"[6] (Figura 2.4); debido al tipo de blindaje realizado, es decir, a la disposición concéntrica de los conductores, el cable coaxial es mucho menos susceptible a interferencias y diafonías que el par trenzado; comparado con éste, el cable coaxial es más pesado y más caro y se puede transportar una gran cantidad de datos sobre largas distancias y es más resistente, así como para conectar un número mayor de estaciones en una línea compartida.

Figura 2.4: Cable Coaxial.



- Velocidad y rendimiento 10 a 100 Mbps.
- Precio económico
- Longitud máxima del cable 500 m.

b) Aplicaciones

Las aplicaciones más importantes del cable coaxial son:

- Distribución de televisión.
- Telefonía a larga distancia.
- Redes de área local.

El cable coaxial se empela para la distribución de TV por cable hasta el domicilio de los usuarios, dicho sistema de TV puede transportar docenas e incluso cientos de canales a decenas de kilómetros.

Tradicionalmente el coaxial ha sido fundamental en la red telefónica de larga distancia, sin embargo actualmente se está utilizando ampliamente la fibra óptica, las microondas terrestre y las comunicaciones vía satélite. "Cuando se utiliza el multiplexaje por división de frecuencia (FDM) el cable coaxial puede transportar más de 10,000 canales de voz simultáneamente"[7].

[6] Idem
[7] Idem

El cable coaxial también es utilizado para conexiones entre periféricos a corta distancia; con señalización digital, el coaxial puede usarse como medio de transmisión en canales de Entrada/Salida (E/S) en computadoras de alta velocidad.

c) Características de Transmisión

El cable coaxial se utiliza para transmitir tanto señales analógicas como digitales, su ancho de banda típico se encuentra entre 400 MHz y 600 MHz, el cual le proporciona al cable coaxial una alta capacidad de transportar datos y una mejor respuesta en frecuencias que el par trenzado, permitiendo mayores frecuencias y velocidades de transmisión. Sus principales limitaciones son la atenuación, el ruido térmico, y el ruido de intermodulación; este último aparece sólo cuando se usan simultáneamente varios canales (FDM) o bandas de frecuencias sobre el mismo cable.

"Para transmisión de señales analógicas a larga distancia se necesitan amplificadores separados entre sí en el orden de pocos kilómetros, estando más alejados cuanto mayor es la frecuencia de trabajo; el espectro de la señalización analógica se extiende hasta aproximadamente 500 MHz. Para señalización digital se necesita un repetidor aproximadamente cada kilómetro, e incluso menos cuanto mayor sea la velocidad de transmisión"[8].

La conexión de dispositivos utilizando cable coaxial debe ser hecha por un profesional, ya que una mala conexión se puede traducir en la inoperabilidad total del sistema.

2.1.3. Fibra Óptica

a) Descripción Física

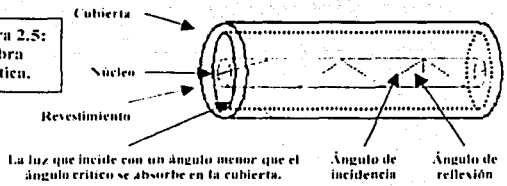
La fibra óptica es un medio flexible y fino capaz de confinar un haz de naturaleza óptica. "Para construir la fibra se pueden usar diversos tipos de cristales y plásticos, se han conseguido pérdidas menores con la utilización de fibras de silicio fundido ultra-puro. Las fibras ultra-puras son muy difíciles de fabricar; las fibras de cristal multicomponente son más económicas, aunque proporcionan unas prestaciones suficientes. La fibra de plástico tiene todavía un costo menor y se puede utilizar para enlaces a cortas distancias para los que son aceptables pérdidas moderadamente altas.

"Un cable de fibra óptica tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta (Figura 2.5). El núcleo es la sección más interna, está constituido por una o varias fibras o hebras muy finas de cristal o plástico y tiene un diámetro entre 8 y 10 μm; cada fibra está rodeada por su propio revestimiento, que no es sino otro cristal o plástico con propiedades ópticas distintas a las del núcleo. La separación entre el núcleo y el revestimiento actúa como un reflector perfecto confinando el haz de luz que de otra manera escaparía del núcleo; la capa más exterior que envuelve a uno o varios revestimientos es la cubierta. La cubierta esta hecha de plástico y otros

[8] Idem

materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, aplastamientos y otros peligros"[9].

Figura 2.5: Fibra Óptica.



- Velocidad y rendimiento 100 Mbps o superior.
- Precio elevado.
- Longitud máxima del cable hasta 2 km.
- Monomodo. Un haz de luz generado por láser.
- Multimodo. Múltiples haces de luz generados por LEDs.

b) Aplicaciones

Existen algunas características diferenciales de la fibra óptica frente al cable coaxial y al par trenzado que son:

- Mayor capacidad. El ancho de banda potencial, y por tanto la velocidad de transmisión en las fibras es enorme; experimentalmente se ha demostrado que se pueden conseguir velocidades de transmisión de cientos de Gbps para decenas de kilómetros de distancia.
- Menor tamaño y peso. Las fibras ópticas son apreciablemente más finas que el cable coaxial o que los pares trenzados embutidos, por lo menos en un orden de magnitud para capacidades de transmisión comparables; la reducción en tamaño conlleva a su vez una reducción en peso, lo que disminuye la infraestructura necesaria.
- Menor atenuación. La atenuación es significativamente menor en la fibras ópticas que en los cables coaxiales y los pares trenzados, además de ser constante en un gran intervalo.
- Aislamiento electromagnético. Los sistemas de fibra óptica no se ven afectados por los efectos de campos electromagnéticos exteriores; estos sistemas no son vulnerables a interferencias, ruido impulsivo o diafonía y por lo tanto las fibras no radian energía, produciendo interferencias despreciables con otros equipos y proporcionando a la vez un alto grado de privacidad.
- Mayor separación entre repetidores. Mientras menos repetidores haya el costo será menor, además de haber menos fuentes de error; desde este punto de vista, las prestaciones de los sistemas de fibra óptica han sido mejoradas de manera constante y progresiva. Para la fibra se necesitan repetidores separados entre sí por docenas de kilómetros, e incluso se ha demostrado experimentalmente sistemas con separación de cientos de kilómetros.

Las 5 aplicaciones básicas en las que la fibra óptica es importante son:

- Transmisiones de larga distancia.
- Transmisiones metropolitanas.

[9] Ídem

- Acceso a áreas rurales.
- Bucles de abonado.
- Redes de área local.

La transmisión de larga distancia mediante fibras es cada vez más común en las redes de telefonía, en dichas redes las distancias medias son aproximadamente 1,500 km y tienen una gran capacidad (normalmente de 20,000 a 60,000 canales de voz). Paralelamente la fibra óptica cada vez se utiliza más como medio de transmisión en cables submarinos.

Los circuitos troncales de alcance metropolitano tienen una longitud media de 12 km y pueden alcanzar hasta 100,000 canales de voz por cada grupo troncal; la mayoría de los servicios se están instalando usando conducciones subterráneas sin repetidores para enlazar centrales telefónicas dentro del área metropolitana.

Los accesos troncales a áreas rurales tienen generalmente longitudes que van desde los 40 a 160 km; en Estados Unidos estos enlaces a su vez conectan frecuentemente centrales telefónicas pertenecientes a diferentes compañías. La mayoría de estos sistemas tienen menos de 5.000 canales de voz.

Los bucles de abonado son fibras que van directamente desde las centrales al abonado. El uso de la fibra en estos servicios está empezando a desplazar a los enlaces mediante pares trenzados y coaxiales dado que cada vez más las redes de telefonía están evolucionando hacia redes integradas capaces de gestionar no sólo voz y datos, sino también imágenes y video.

Finalmente, una aplicación importante de la fibra óptica está en las redes de área local. Recientemente se han desarrollado estándares y productos para redes de fibra óptica con capacidades que van desde 100 Mbps hasta 1 Gbps y a su vez permiten cientos, incluso miles de estaciones en grandes edificios de oficinas.

c) Características de Transmisión

"La fibra óptica propaga el haz de luz internamente de acuerdo con el principio de reflexión total; este fenómeno se da en cualquier medio transparente que tenga un índice de refracción mayor que el medio que lo contenga. La fibra óptica funciona como una guía de ondas para el rango de frecuencias que va desde 10^{14} hasta 10^{15} Hz, cubriendo parte del espectro visible e infrarrojo"[10].

La luz proveniente de la fuente penetra en el núcleo cilíndrico de cristal o plástico; los rayos que inciden con ángulos superficiales se reflejan y se propagan dentro del núcleo de la fibra, mientras que para otros ángulos los rayos son absorbidos por el material que forma el revestimiento. Este tipo de propagación se llama multimodal o de índice discreto (Figura 2.6a), lo que alude al hecho de que hay multitud de ángulos para los que se da la reflexión total; el cable tiene un radio aproximado de 30 a 70 micrones. En la transmisión multimodo existen múltiples caminos que verifican la reflexión total, cada uno con

[10] Idem

diferente longitud y por tanto con diferente tiempo de propagación, lo cual hace que los elementos que se transmitan (pulsos de luz) se dispersen en el tiempo, limitando la velocidad a la que los datos pueden ser correctamente recibidos; dicho de otra forma, la necesidad de separar los pulsos de luz limita la velocidad de trasmisión de los datos. Este tipo de fibra es más adecuada para la transmisión en distancias cortas. Cuando el radio del núcleo se reduce, la reflexión total se dará en un menor número de ángulos.

Si se reduce el radio del núcleo a dimensiones del orden de magnitud de la longitud de onda, un solo ángulo o modo podrá pasar: el rayo axial: esta propagación monomodo (Figura 2.6c) proporciona prestaciones superiores. Debido a la existencia de un único camino posible en la transmisión monomodo la distorsión multimodal no puede darse. Las fibras monomodo se utilizan normalmente en aplicaciones de larga distancia como la telefonía y la televisión por cable. En la transmisión monomodo el núcleo de la fibra tiene un radio de entre 2.5 a 4 micrones.

Se puede conseguir un tercer modo de transmisión variando gradualmente el índice de refracción del núcleo, denominado multimodo de índice gradual (Figura 2.6b), sus características se encuentran entre las de los otros dos modos anteriores. "Estas fibras disponen de un índice de refracción superior en la parte central, lo que hace que los rayos de luz avancen más rápidamente conforme se alejan del eje axial de la fibra, en lugar de describir un zig-zag, la luz en el núcleo describe curvas helicoidales debido a la variación gradual del índice de refracción, reduciendo así la distorsión multimodal"[11]. El efecto de la mayor velocidad de propagación en la periferia del núcleo se traduce en que aún recorriendo distancias superiores, todos los rayos llegan aproximadamente en los mismos. Este tipo de fibras de índice gradual se utilizan en las redes de área local y el cable tiene un radio de 25 a 60 micrones.

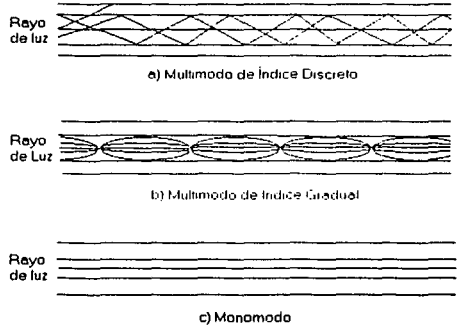


Figura 2.6: Modos de Transmisión en las Fibras Ópticas.

[11] Idem

"En los sistemas de fibra óptica se usan dos tipos diferentes de fuentes de luz: los diodos LED (Light Emitting Diode) y los diodos ILD (Injection Laser Diode). Ambos son dispositivos semiconductores que emiten un haz de luz cuando se les aplica una tensión"[12]: el LED es menos costoso, opera en un rango mayor de temperaturas y tiene una vida media superior. El ILD, cuyo funcionamiento está basado en el mismo principio que el láser, es más eficaz y puede proporcionar velocidades de transmision superiores.

Existe una relación entre la longitud de onda utilizada, el tipo de transmisión y la velocidad de transmisión que se puede conseguir. Tanto el monomodo como el multimodo pueden admitir varias longitudes de onda diferentes y pueden utilizar como fuentes tanto láseres como diodos LED. En las fibras ópticas, la luz se propaga mejor en tres regiones de longitudes de onda, centradas a 850, 1,300 y 1,500 nanómentros (nm). Las pérdidas son menores cuanto mayor es la longitud de onda, permitiendo así mayores velocidades de transmisión sobre distancias superiores. En la actualidad la mayoría de las aplicaciones usan como fuentes diodos LED a 850 nm.

La fibra óptica tiene un ancho de banda de entre 1014 a 1015 Hz. Con un ancho de banda mucho mayor que cualquier otro tipo de cable, una fibra óptica puede transportar la señal de miles de conversaciones telefónicas simultáneas, además puede transportar señales más rápidamente y sin distorsión que cualquier otro esquema de cableado.

Para redes de área local las fibras pueden transportar datos aproximadamente a la misma velocidad que el cable coaxial, sin embargo la fibra óptica puede transportar los datos de forma más confiable y segura que cualquier otro tipo de medio. Además la fibra tiene el potencial de transportar datos a mayores velocidades de acuerdo al desarrollo tecnológico actual.

"La fibra óptica tiene beneficios adicionales relativos a la seguridad. Las señales eléctricas que viajan en un cable coaxial o en un par trenzado pueden ser detectadas ya que emiten radiación electromagnética, la cual, con el equipo adecuado, puede ser usada para obtener el mensaje original. Por otro lado, la luz no emite radiación electromagnética, así es que es más difícil para usuarios no autorizados obtener la señal en una fibra"[13].

2.2. Medios de Transmisión no Guiados

Los medios de transmisión no guiados utilizan antenas para la transmisión y recepción de las señales, entre los diferentes tipos de señales que pueden ser transmitidas utilizando este formato se encuentran las microondas y las señales vía satélite. Un rayo de microondas puede concentrarse hacia una dirección en donde se localiza una antena receptora. "La habilidad de enfocar una ráfaga de señales en un medio no guiado depende de la frecuencia de las señales transmitidas. La frecuencia de una señal es el número de ciclos de una señal por segundo, es decir el número de veces que la señal varía en un

[12] Idem
[13] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Primer Año".

segundo"[14]. Conforme la frecuencia sea mayor será más fácil enfocar la ráfaga en una dirección específica.

En medios no guiados, tanto la transmisión como la recepción se lleva a cabo mediante antenas: en la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire) y en la recepción la antena capta las ondas electromagnéticas del medio que la rodea. "Básicamente en las transmisiones inalámbricas hay dos tipos de configuraciones: direccional y omnidireccional. En la primera, la antena de transmisión emite la energía electromagnética concentrándola en un haz, por ello las antenas de emisión y recepción deben estar perfectamente alineadas. En el caso omnidireccional el diagrama de radiación de la antena es más disperso, emitiendo en todas direcciones y la señal puede ser recibida por varias antenas"[15]. En general, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

En el estudio de las comunicaciones inalámbricas se consideran tres rangos de frecuencias. "El primer intervalo definido desde los 2 GHz (1 GHZ = 10^9 Hertz) hasta los 40 GHz se denomina frecuencias de microondas; en estas frecuencias de trabajo se pueden conseguir haces altamente direccionales, por lo que las microondas son adecuadas para enlaces punto a punto; también se utilizan para las comunicaciones vía satélite. Las frecuencias que van desde 30 MHz a 1 GHz son adecuadas para las aplicaciones omnidireccionales, a este rango de frecuencias se denomina intervalo de ondas de radio.

Otro rango de frecuencias importante para las aplicaciones de cobertura local es la zona del espectro de infrarrojos definida aproximadamente por el rango de frecuencias comprendido entre 3 X 10^{11} hasta 2 X 10^{14} Hz"[16]. Los infrarrojos son útiles para las conexiones locales punto a punto, así como para aplicaciones multipunto dentro de áreas de cobertura limitada.

2.2.1. Microondas Terrestres

a) Descripción Física

"La antena más común en las microondas es la de tipo parabólico; su tamaño típico es de un diámetro de unos 3 metros, esta antena es rígidamente fija y el haz estrecho debe estar perfectamente enfocado hacia la antena receptora (Figura 2.7). Las antenas de microondas se sitúan a una altura apreciable sobre le nivel del suelo, con el fin de conseguir mayores separaciones entre ellas y para evitar posibles obstáculos en la transmisión. Si no hay obstáculos intermedios la distancia máxima entre antenas es

$$d=7.14\sqrt{Kh}$$

donde d es la distancia de separación entre las antenas expresada en kilómetros, h es la altura de la antena en metros y K es el factor de corrección que tiene en cuenta que las

[14] Idem
[15] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".
[16] Idem

microondas se desvían o refractan con la curvatura de la tierra llegando, por lo tanto, más lejos de lo que lo harían si se propagaran en línea recta. Una buena aproximación es considerar K = 4/3"[17]. Por lo tanto, a modo de ejemplo, dos antenas de microondas con altura de 100 metros pueden separarse una distancia igual a 7.14 x √133 = 82 km.

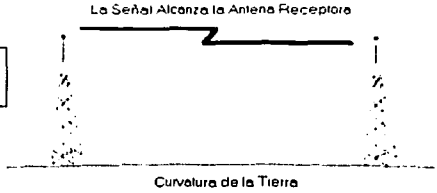


Figura 2.7:
Microondas Terrestres.

EL propósito principal de las torres de microondas es conectar computadoras o equipos de comunicaciones localizados en diferentes áreas geográficas; por ejemplo una compañía que tiene varias oficinas distribuidas a lo largo de una ciudad podría utilizar microondas para conectar todo su equipo de procesamiento de datos.

b) Aplicaciones

El uso principal de los sistemas de microondas terrestres son los servicios de telecomunicaciones de larga distancia; para una distancia dada, las microondas requieren menor número de repetidores o amplificadores que el cable coaxial y por el contrario necesita que las antenas estén perfectamente alineadas. El uso de las microondas es frecuente en la transmisión de televisión y de voz.

Otro uso cada vez más frecuente es en enlaces punto a punto entre edificios en distancias cortas; en este caso, las aplicaciones típicas son circuitos cerrados de TV o la interconexión de redes locales, además las microondas en distancias cortas también se utilizan en las aplicaciones denominadas "bypass", con las que una determinada compañía puede establecer un enlace privado hasta el centro proveedor de transmisiones de larga distancia, evitando así tener que contratar el servicio a la compañía telefónica local.

Dependiendo de la cantidad de equipo que se desea conectar, el flujo de datos y las necesidades de procesamiento de la compañía, puede ser una buena inversión establecer un sistema de comunicaciones con microondas para resolver sus necesidades de comunicación.

c) Características de Transmisión

El rango de las microondas cubre una parte sustancial del espectro electromagnético, la banda de frecuencias está comprendida entre los 2 y 40 GHz; cuanto mayor sea la frecuencia utilizada mayor es el ancho de banda potencial, y por tanto mayor es la posible velocidad de transmisión; "aunque la tasa de transmisión de datos se

[17] Idem

incrementa, la atenuación de la señal también se incrementa, es por ello que las altas frecuencias se utilizan solamente para transmisiones a corta distancia"[18]. Estas frecuencias están subdivididas en varias áreas de transmisión de datos.

Al igual que en cualquier sistema de transmisión, "la principal causa de pérdidas en las microondas es la atenuación. Las pérdidas se pueden expresar como:

$$L=10\log\left(\frac{4\pi d}{\lambda}\right)^2 \text{ dB}$$

donde d es la distancia y λ es la longitud de onda, expresadas en las mismas unidades"[19]. Por lo tanto en los sistemas que usan microondas, los amplificadores o repetidores se pueden distanciar más (de 10 a 100 km generalmente) que en coaxiales y pares trenzados. La atenuación aumenta con las lluvias, siendo este efecto especialmente significativo para frecuencias por encima de 10 GHz; otra dificultad adicional son las interferencias. Con la popularidad creciente de las microondas, las áreas de cobertura se pueden solapar, haciendo que las interferencias sean siempre un peligro potencial; así pues la asignación de bandas tiene que realizarse siguiendo una estricta regulación.

Las bandas más usuales en la transmisión a larga distancia se sitúan entre 4 GHz y 6 GHz. Debido a la creciente congestión que están sufriendo dichas bandas, la banda de 11 GHz se está empezando a utilizar. La banda de 12 GHz se usa para proporcionar la señal de TV a las cabeceras de distribución de TV por cable, en las que para llegar al abonado se utiliza el cable coaxial. Finalmente, cabe citar que las microondas de alta frecuencia se están utilizando para enlaces cortos punto a punto entre edificios, utilizando la banda de 22 GHz. A frecuencias superiores, las antenas son más pequeñas y más baratas.

Las microondas ofrecen buena velocidad, costo efectivo (debido a que no existe cableado) y una sencilla operación; sin embargo pueden existir interferencias con las ondas de radio. Además las transmisiones comerciales pueden ser interpretadas por cualquier persona que tenga un receptor en la línea de transmisión; sin embargo y a pesar de todos sus inconvenientes, las microondas son una solución popular a los problemas y necesidades de la comunicación de datos.

2.2.2. Microondas por Satélite

a) Descripción Física

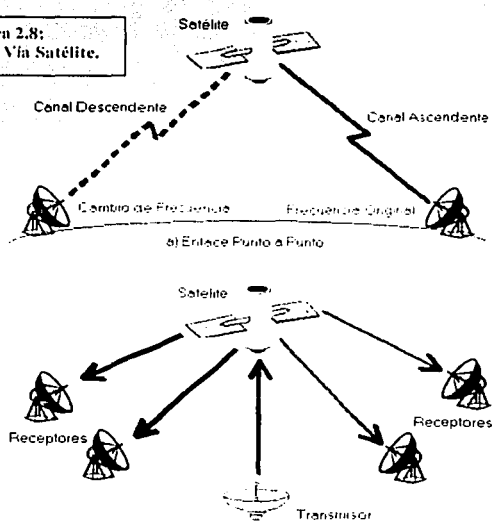
La transmisión vía satélite es similar a la transmisión a través de microondas, pero en lugar de transmitir a una estación receptora terrestre, se transmite a un satélite ubicado a varias miles de millas de distancia en el espacio exterior (aproximadamente 22,300 millas). Sus componentes básicos son una estación terrestre, utilizada para enviar y recibir los datos y un satélite.

[18] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Primer Año".
[19] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

Un satélite de comunicaciones es esencialmente una estación que transmite microondas, utilizado como enlace entre dos o más receptores/transmisores terrestres, denominados estaciones base. El satélite recibe la señal en una banda de frecuencia (canal ascendente), la amplifica o repite, y posteriormente la retransmite en otra banda de frecuencia (canal descendente); cada uno de los satélites geoestacionarios operará en una serie de bandas de frecuencias llamadas "transponder channels" o simplemente "transponders".

El satélite se puede utilizar para proporcionar un enlace punto a punto entre dos antenas terrestres alejadas entre sí, o bien para conectar una estación base transmisora con un conjunto de receptores terrestres (Figura 2.8).

Figura 2.8: Microondas Vía Satélite.



Para que un satélite de comunicaciones funcione con eficacia, generalmente se exige que se mantenga en una órbita geoestacionaria, es decir que mantenga una posición respecto a la tierra, de no ser así, no estaría constantemente alineado con las estaciones base. "El satélite para mantenerse geoestacionario debe tener un período de rotación igual al de la tierra y esto sólo ocurre a una distancia de 35,784 km.

Si dos satélites utilizaran la misma banda de frecuencias y estuvieran suficientemente próximos, podrían interferirse mutuamente, para evitar esto los estándares actuales exigen una separación mínima de 4° (desplazamiento angular medio desde la superficie terrestre) en la banda 4/6 GHz, y una separación de al menos 3° a 12/14 GHz, por lo tanto el número máximo posible de satélites está bastante limitado"[20].

b) Aplicaciones

Entre las aplicaciones más importantes para los satélites cabe destacar:

- La difusión de la televisión.
- La transmisión telefónica de larga distancia.
- Las redes privadas.

Debido a que los satélites son multidestino por naturaleza, su utilización es muy adecuada para la distribución de TV. La PBS (Public Broadcasting Service) es una red que distribuye su programación casi exclusivamente mediante el uso de los canales de satélite; otras redes comerciales también utilizan el satélite como parte esencial de su sistema, al igual que los sistemas de distribución de TV por cable lo utilizan como medio para obtener su programación. "La aplicación más reciente de la tecnología del satélite a la televisión es la denominada difusión directa vía satélite (DBS, Direct Broadcast Satellite), en la que la señal de video se transmite directamente desde el satélite a los domicilios de los usuarios"[21].

La transmisión vía satélite se utiliza también para proporcionar enlaces punto a punto entre las centrales telefónicas en las redes públicas de telefonía; es el medio óptimo para los enlaces internacionales que tengan un alto grado de utilización y es competitivo comparado con los sistemas terrestres en muchos enlaces internacionales de larga distancia.

Para la tecnología vía satélite hay una gran cantidad de aplicaciones de gran interés comercial; el suministrador del servicio de transmisión vía satélite puede dividir la capacidad total disponible en una serie de canales, alquilando su uso a terceras persona; dichas compañías equipadas con una serie de antenas distribuidas en diferentes localizaciones pueden utilizar un canal del satélite para establecer una red privada. Tradicionalmente, tales aplicaciones eran bastante caras, limitando su uso a las grandes empresas.

c) Características de Transmisión

"El rango de frecuencias óptimo para la transmisión vía satélite está en el intervalo comprendido entre 1 y 10 GHz, el ruido producido por causas naturales es apreciable, incluyendo el ruido galáctico, solar, atmosférico y el producido por interferencias con otros dispositivos electrónicos; por encima de los 10 GHz, la señal se ve severamente afectada por la absorción atmosférica y por las precipitaciones.

[20] Ídem
[21] Ídem

La mayoría de los satélites que proporcionan servicio de enlace punto a punto operan en el intervalo de 5.925 y 6.425 GHz para la transmisión desde el satélite hasta la tierra (canal descendente), conocida como banda 4/6 GHz"[22]. En una transmisión continua y sin interferencias, el satélite no podrá transmitir y recibir en el mismo rango de frecuencias; así pues, las señales que se reciben desde las estaciones terrestres en una frecuencia dada se deberán devolver en otra distinta. Conforme el valor de la frecuencia disminuye, el tamaño de la antena requerida para recibir y transmitir las señales aumenta.

"La banda 4/6 GHz está dentro de la zona óptima de frecuencias (de 1 a 10 GHz), pero su exhaustiva utilización ha llegado a la saturación de estas frecuencias; por ello se han desarrollado otras bandas alternativas como es la 12/14 GHz (el canal ascendente está situado entre 14 y 14.5 GHz y la banda descendente está entre 11.7 y 14.2 GHz); en esta banda aparecen problemas de atenuación que se deben solventar, no obstante, se pueden usar receptores terrestres más baratos y de dimensiones más reducidas. Se ha diagnosticado que esta banda también se saturará, por lo que se está proyectando la utilización de la banda 19/29 (enlace ascendente de 27.5 a 31.0 GHz, enlace descendente de 17.7 a 21.2 GHz), en dicha banda la atenuación es incluso superior, sin embargo proporcionará un ancho de banda mayor (2.500 MHz) a la vez que los receptores pueden ser todavía más pequeños y económicos"[23].

La seguridad es un problema en las comunicaciones vía satélite debido a que es fácil interceptar la transmisión que viaja a través del aire; en algunos casos se utiliza un dispositivo para distorsionar la señal antes de que se envíe al satélite y un dispositivo capaz de reproducir la señal original en la estación receptora.

Algunas propiedades peculiares de las comunicaciones vía satélite son:

- Debido a las grandes distancias involucradas hay un retardo de propagación aproximado del orden de un cuarto de segundo para la transmisión desde una estación terrestre hasta otra pasando por el satélite; este retardo es significativo si se trata de una conversación telefónica ordinaria, además estos retrasos introducen problemas adicionales a la hora de controlar los errores y el flujo en la transmisión. Asimismo existe un retardo adicional debido al tiempo que requiere la señal para viajar a través de las estaciones terrestres.
- Los satélites con microondas son intrínsicamente un medio para aplicaciones multidestino; varias estaciones pueden transmitir hacia el satélite e igualmente varias estaciones pueden recibir la señal transmitida por el satélite.
- El satélite debe estar alineado con las estaciones terrestres.

2.2.3. Ondas de Radio

La diferencia más apreciable entre las microondas y las ondas de radio es que éstas últimas son omnidireccionales, mientras que las primeras tienen un diagrama de radiación

[22] Ídem
[23] Ídem

mucho más direccional, por lo tanto las ondas de radio no necesitan antenas parabólicas, ni necesitan que dichas antenas estén instaladas sobre una plataforma rígida para estar alineadas.

a) Aplicaciones

"Con el término radio se alude a una manera poco precisa a toda la banda de frecuencias desde 3KHz a 300 GHz. Se utiliza de manera informal el término "ondas de radio" para aludir a la banda VHF (Very High Frecuency) y parte de la UHF (Ultra High Frecuency) entre el rango de 30 MHz a 1 GHz; este rango también cubre la frecuencia de la radio comercial; a su vez se utiliza para una serie de aplicaciones de redes de datos"[24].

La transmisión de radio celular es una forma de transmitir señales de radio a altas frecuencias donde las señales son transmitidas desde las antenas que se encuentran colocadas en lugares estratégicos a través de áreas metropolitanas.

Cada área de servicio está dividida en pequeñas células y cada una tiene un sitio de transmisión y recepción fijo. Si una persona está haciendo una llamada y se mueve a la orilla de la célula actual, automáticamente el sistema celular de radio mueve la comunicación del usuario a otra antena más cercana; de esta manera la transmisión no se interrumpe y el usuario no tiene que preocuparse por moverse de una célula a otra.

"La transmisión de radio celular puede utilizarse para comunicaciones de voz o datos. En el sistema celular, cuando un usuario desea realizar una transmisión, la voz o los datos son enviados directamente desde la ubicación actual del usuario a la antena de la célula correspondiente, la cual transmite la información a través de un área de servicio o en algunos casos los datos pueden ser transmitidos a un satélite para comunicaciones de larga distancia"[25].

Varias laptops y palmtops cuentan con capacidades de transmisión de radio celular, lo que le permite a un usuario en cualquier sitio marcar a un sitio central para descargar o actualizar datos, liberando al emisor de localizar un teléfono y comunicarse de forma tradicional.

b) Características de Transmisión

El rango de frecuencias comprendido entre 30 MHz y 1 GHz es muy adecuado para la transmisión simultánea a varios destinos; a diferencia de las ondas electromagnéticas con frecuencias menores, la ionosfera es transparente para ondas con frecuencias superiores a 30 MHz. Así pues, la transmisión es posible cuando las antenas están alineadas sin producirse interferencias entre los transmisores debidas a las reflexiones con la atmósfera. A diferencia de la región de las microondas, las ondas de radio son menos sensibles a la atenuación producida por la lluvia.

[24] Ídem
[25] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Primer Año".

"La distancia máxima entre el transmisor y el receptor es ligeramente mayor que el alcance visual, es decir, $7.14\sqrt{Kh}$. Al igual que las microondas, la atenuación debida simplemente a la distancia es igual a $10 \log \left(\frac{4\pi d}{\lambda} \right)^2$. Debido a que tienen una longitud de onda mayor, las ondas de radio sufren, en términos relativos una menor atenuación"[26].

Un factor determinante en las ondas de radio son las interferencias por multitrayectorias. Entre las antenas, debido a la reflexión en la superficie terrestre, el mar u otros objetos, pueden aparecer multitrayectorias; este efecto se observa con frecuencia en el receptor de TV y consiste en que se pueden observar varias imágenes o sombras cuando pasa un avión por el espacio cercano.

2.2.4. Infrarrojos

Las comunicaciones mediante infrarrojos se llevan a cabo a través de transmisores/receptores (transceivers) que modulan luz infrarroja no coherente. Los transceivers deben estar bien alineados directamente o mediante la reflexión de una superficie coloreada como puede ser el techo de una habitación.

Una diferencia significativa entre la transmisión de rayos infrarrojos y las microondas es que los primeros no pueden atravesar las paredes, por lo tanto los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este tipo de transmisión, es más, no hay problemas de asignación de frecuencias, ya que en esta banda no se necesitan permisos.

[26] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

CAPÍTULO 3

Tecnologías de Interconectividad de Redes

3.1. Topologías de Red

Una configuración de red se denomina topología de red, la cual establece la forma física y lógica de la red. El diseñador de una red tiene tres objetivos al establecer la topología de la misma:

- Proporcionar la máxima fiabilidad a la hora de establecer el tráfico.
- Direccionar el tráfico utilizando la vía del costo mínimo entre el transmisor y el receptor.
- Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo.

El concepto de fiabilidad hace referencia a la capacidad de enviar los datos correctamente (sin errores) entre los equipos terminales, involucra la posibilidad de la recuperación de errores o de datos perdidos en la red por motivos de fallas en el medio: también tiene que ver con el mantenimiento del sistema: pruebas diarias, sustitución de componentes defectuosos y en su caso aislamiento de fallas.

La segunda meta al establecer una topología de red es proporcionar el camino de costo mínimo entre los procesos de aplicación que residen en los equipos terminales, para ello se requiere lo siguiente:

1. Minimizar la longitud real de la ruta entre los componentes que se comunican, para lo cual se debe direccionar el tráfico pasando por el menor número posible de componentes intermedios.
2. Proporcionar el medio más barato para una aplicación determinada.

El tercer objetivo de interés al establecer un topología es proporcionar el tiempo mínimo de respuesta y el máximo rendimiento. Para minimizar el tiempo de respuesta hay que procurar minimizar el retardo entre la transmisión y la recepción de datos entre las terminales; el rendimiento tiene que ver con la transmisión de la máxima cantidad de datos en un período determinado.

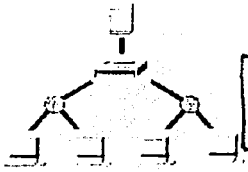
3.1.1. Topología Jerárquica

La topología jerárquica (red vertical o red de árbol) es una de las topologías más utilizadas hoy en día, el software para controlar la red es relativamente simple y la propia topología proporciona un punto de concentración para el control y resolución de errores.

Existe una simplicidad en el control, pero presenta serios problemas de cuello de botella. La computadora colocada en la raíz de la jerarquía es la encargada de controlar el tráfico generado por los demás equipos. Además existe el problema de la fiabilidad, ya que en el caso de una falla en la máquina situada en la raíz, la red quedaría completamente fuera de servicio a no ser que otro nodo asuma las funciones del nodo defectuoso.

"Existe un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor"[1] (Figura 3.1).

Figura 3.1: Topología Jerárquica.



3.1.2. Topología Horizontal (Bus)

Es una disposición muy popular en redes de área local; el control del tráfico entre las computadoras es relativamente simple, ya que el bus permite que todas las estaciones reciban la transmisión, es decir, cada estación puede difundir la información a todas las demás; sólo existe un único canal de comunicaciones al que se conectan todos los dispositivos de la red, en consecuencia si dicho canal falla, la red deja de funcionar. Otro problema que presenta esta configuración es la dificultad de aislar los componentes defectuosos conectados al bus debido a la ausencia de puntos de concentración.

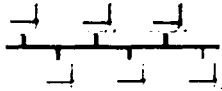
La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre ellos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados (Figura 3.2).

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si se desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja

[1] Black, Uyless. 1997. Ed. AlfaOmega. "Redes de Computadoras, Protocolos, Normas e Interfaces".

ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden solucionar segmentando la red en varias partes.

Figura 3.2: Topología de Bus.



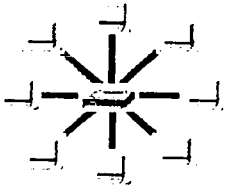
3.1.3. Topología de Estrella

Es ampliamente utilizada en sistemas de comunicación de datos. La red de estrella fue muy utilizada durante los años 1960 y 1970 debido a que era sencilla de controlar: el software no es complicado, el flujo de tráfico es simple; todo el tráfico surge del centro de la estrella. Una sola computadora controla completamente a los demás dispositivos conectados a ella; por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula a través de la red (Figura 3.3). Por lo tanto es una estructura muy semejante a la estructura jerárquica, con la diferencia que en la topología de estrella se tienen mucho más limitadas las posibilidades de procesamiento distribuido.

"La computadora principal tiene la responsabilidad de direccionar el tráfico entre los otros componentes, también es responsable de ocuparse de las fallas. Debido a que existe un equipo central esta topología sufre de cuellos de botella y las fallas en el nodo central repercuten en la mala operación de la red"[2].

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

Figura 3.3: Topología de Estrella.



3.1.4. Topología de Anillo

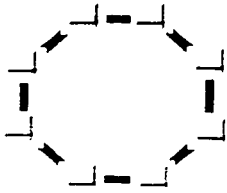
La topología de anillo recibe su nombre del aspecto circular del flujo de datos, en muchos casos, el flujo de datos va en una sola dirección, es decir, una máquina recibe la señal y la envía a la siguiente estación del anillo, los cuellos de botella son muy raros y la lógica necesaria en una red de este tipo es relativamente simple. Las tareas que debe

[2] Ídem

realizar cada componente son aceptar los datos, enviarlos al siguiente equipo que se encuentra conectado con él, o bien enviarlos al siguiente componente intermedio en el anillo. Su principal inconveniente es que un único canal une a todos los componentes del anillo. Si falla el canal entre dos nodos, falla toda la red.

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces en el que cada nodo está conectado solamente con los dos nodos adyacentes (Figura 3.4). Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

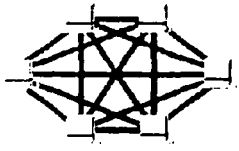
Figura 3.4:
Topología de Anillo.



3.1.5. Topología en Malla

Su principal atractivo es su relativa inmunidad a problemas de fallas y cuellos de botella. Dada la multiplicidad de caminos entre los equipos terminales es posible direccionar el tráfico evitando componentes que presenten alguna falla o nodos ocupados; aunque esta solución es costosa, algunos usuarios prefieren la gran confiabilidad que esta topología ofrece en comparación con las demás.

Figura 3.5:
Topología en Malla.



En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como todo se conecta físicamente a los demás nodos, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a su destino (Figura 3.5). Además, esta topología permite que la información circule por varias rutas a través de la red. La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos,

ya que de lo contrario la cantidad de medios necesarios para los enlaces y la cantidad de conexiones entre los nodos se tornaría abrumadora.

3.2. Tecnologías LAN (Local Area Network)

3.2.1. Ethernet

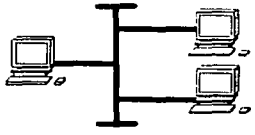
"La tecnología Ethernet es la mas usada en la actualidad, su primera implantación fue en la compañía Xerox por Robert Matcalfe a principios de 1970, para conectar hasta 100 computadoras en un área de 100 km, con una transferencia de información de 2.94 Mbps"[3].

En 1978 se publicó la primera norma, como un trabajo conjunto de las empresas Digital, Intel y Xerox, ésta es la base del estándar ANSI/IEEE 802.3 (American National Standards Institute/ Institute of Electrical and Electronics Engineers) publicado en 1983 por la IEEE.

La tecnología Ethernet se utiliza principalmente en topologías de Bus y de Estrella. El método de acceso al medio físico es CSMA/CD (Carrier Sense Multiple Access with Collision Detection), el cual funciona de tal forma que primero se tiene que escuchar el medio para asegurar que nadie está transmitiendo en ese momento; si nadie lo está haciendo comienza la transmisión. Por otro lado, en el caso de que el medio esté siendo ocupado por otro dispositivo, se espera un tiempo aleatorio y después se vuelve a intentar la transmisión.

"Si llegara a suceder que dos dispositivos escucharan el canal al mismo tiempo y comenzaran a transmitir, la información chocaría en algún punto de la red, lo que originaría una colisión. Esto se debe a que existen tiempos de propagación de la información, por lo que el dispositivo no solo escucha el canal para poder transmitir información, sino que también lo hace mientras está transmitiendo y cuando se llevan a cabo colisiones; por ello cada dispositivo puede transmitir su información, pero antes de hacerlo espera un tiempo aleatorio dado por un algoritmo, con lo que se minimiza el número de colisiones en una red"[4].

Figura 3.6: Segmento Ethernet.



[3] Rodríguez, G. y E., Jorge. 1996. Ed. McGraw-Hill. "Introducción a las Redes de Área Local".
[4] Ídem.

a) Formato de la Trama

Ethernet utiliza un tipo de señalización conocido como codificación Manchester (Figura 3.7), que garantiza que por cada bit transmitido ocurra una transición del nivel lógico de la señal.

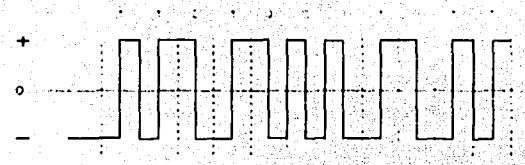


Figura 3.7: Codificación Manchester.

La forma en que las redes Ethernet transmiten datos se llama datagrama o trama (Figura 3.8). La información que se envía del emisor al receptor se pone en datagramas y cada datagrama contiene parte de la información. La información que viaja en cada trama que se transmite en la red es la siguiente:

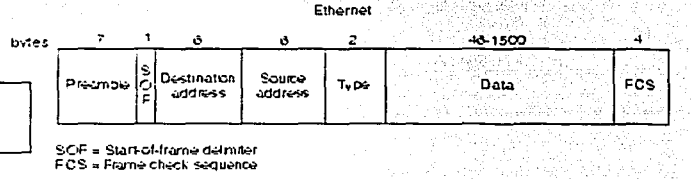


Figura 3.8: Trama Ethernet.

- Preamble (Preámbulo). Campo de 7 bytes con el código 10101010 (Figura 3.9). Al transmitir estos bytes en la codificación Manchester, se genera una señal cuadrada que sirve para sincronizar a los receptores en la red.

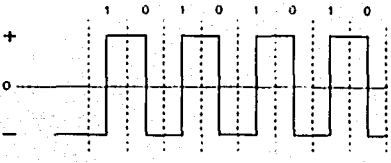
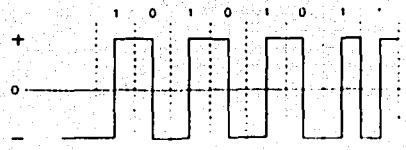


Figura 3.9: Campo de Preámbulo.

- SOF (Start of Frame Delimiter), Delimitador de Comienzo. Es un byte formado por el patrón 10101011 (Figura 3.10). El último par de bits interrumpe la onda cuadrada formada por el preámbulo y los primeros bits de este byte; esta interrupción sirve para indicar donde se inician en realidad los campos de información útil.

Figura 3.10: Campo de SOF.



- Destination Address (Dirección Destino). Este campo contiene información de la dirección MAC (Media Access Control), que es única para toda la red debido a que está formada por 6 bytes, de los cuales los 3 primeros pertenecen al código de la compañía que produce las tarjetas de red y los 3 restantes son el número de serie de la misma. La dirección de destino puede ser de unicast, multicast o broadcast.

- Source Address (Dirección Origen). Contiene la dirección MAC de la computadora que originó la trama. La dirección de origen es siempre una dirección de unicast.

- Type (Tipo). Para Ethernet este campo determina que tipo de trama es la que se está enviando: puede ser una trama IP con valor 0800, o X.25 con valor 0805, etc. En otras palabras especifica el protocolo de la capa superior que recibe los datos una vez terminado el procesamiento de Ethernet.

- Data (Información). Terminado el procesamiento de la capa física y de la capa de enlace de datos, la información que se desea transmitir contenida en este campo se envía hacia un protocolo de las capas superiores identificado en al campo "Type". La cantidad mínima de la trama es de 64 bytes y la máxima de 1518, esto se debe a que el método de acceso no garantiza una igualdad en la utilización del canal. Dentro de este campo también viaja información relacionada con el protocolo de comunicaciones que se esté utilizando.

- FCS (Frame Check Sequence), Secuencia de Verificación de Trama. El último campo es un código de redundancia cíclica de 32 bits (4 bytes) y está formado por el cálculo o la aplicación de un algoritmo sobre los campos de Source Address, Destination Address, Type y Data. Este campo sirve para verificar que la información que se envía sea la misma que se recibe; el algoritmo de verificación se ejecuta antes de enviar la trama y al momento de recibirla.

b) Características

- El método de acceso al medio CSMA/CD no garantiza un tiempo de respuesta determinístico debido a que todos los dispositivos que están integrados a la red compiten por el mismo medio, lo que hace que el tiempo de respuesta sea probabilístico.

- Debido a que existe un tamaño mínimo de trama (64 bytes), el hecho de transmitir tramas de control que ocupen menos de los 64 bytes ocasiona un desperdicio en el ancho de banda del medio.
- El desempeño de la red está en función del número de dispositivos que se conecten a la misma. El tráfico que se genere en una red Ethernet, según estadísticas, no debe exceder el 40% de utilización del ancho de banda total.
- Las redes Ethernet son una tecnología madura
- Su operación es relativamente sencilla y su método de acceso al medio es aceptable en cargas de trabajo pequeñas.
- Ethernet es el tipo de red idónea en ambientes heterogéneos.
- Es flexible a los cambios en la configuración de la red.

La tecnología Ethernet es una de las más antiguas y sencillas que existen en nuestros días y se ha ido adaptando a los cambios tecnológicos de hoy en día. Actualmente existe las tecnología FastEthernet que permite velocidades de 100 Mbps y recientemente surgió la tecnología GigabitEthernet que permite velocidades de 1 Gbps, ambas tecnologías pueden ser implantadas tanto con fibra óptica como con cable UTP.

Cada una de las computadoras que se encuentran en la red tiene una tarjeta de red lo que permite utilizar el método de acceso al medio. Cada tarjeta de red es la encargada de manejar las colisiones y controlar la codificación como la decodificación de la señal.

"Un segmento de red Ethernet tiene una capacidad máxima de 100 nodos y pueden ser interconectados múltiples segmentos con el uso de switches. En una red Ethernet no pueden existir más de 4 switches y 5 segmentos de red, de los cuales dos segmentos son solamente de intercambio de información"[5].

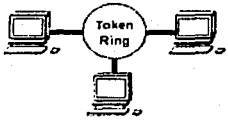
3.2.2. Token Ring

Cuando IBM (International Business Machines) colocó en el mercado las redes Token Ring, inmediatamente se convirtió en el competidor número 1 de las redes Ethernet 802.3. El comité de la IEEE 802.5 ha desarrollado estándares para las redes Token Ring, así como algunos de sus componentes.

"Las redes Token Ring son deterministicas, el método de acceso al medio que utiliza esta tecnología se conoce como Token Passing, el cual está diseñado para operar en redes con topología de anillo, aunque físicamente son cableadas en forma de estrella utilizando una unidad MSAU (Multistation Access Unit)"[6] (Figura 3.11). Las computadoras transmiten la información en paquetes llamados Tramas. El comité 802.5 publicó un conjunto de especificaciones sobre la trama Token Ring; originalmente esta tecnología transmitía a 4 Mbps, pero después de varios años, un conjunto de empresas incluida IBM, logró alcanzar velocidades de 16 Mbps.

[5] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Primer Año".
[6] Rodríguez, G. y E., Jorge. 1996. Ed. McGraw-Hill. "Introducción a las Redes de Área Local".

Figura 3.11: Red Token Ring.



La forma en que la información viaja de una estación a otra es por medio de un "token" (testigo). El token es el mecanismo a través del cual se puede transmitir la información. Si una computadora posee el token, puede transmitir; si no cuenta con él tiene que esperar su turno. Debido a que la información viaja en forma de anillo, el token recorre cada una de las estaciones conectadas a él, de tal forma que al momento de recibirlo cada una de las estaciones lee el paquete para ver si le corresponde, en caso negativo, lo transmite al anillo de la misma forma en que trabaja un repetidor, por lo que cada vez que una computadora lee el mensaje y lo regresa a la red, es un paquete nuevo con la misma información. Este proceso de leer y enviar un paquete es lo que determina que no exista un número máximo de nodos conectados al anillo.

Cuando el token regresa a la computadora que originó el mensaje, ésta verifica que la información haya sido entregada correctamente y entonces libera el token a la siguiente máquina; debido a este fenómeno es posible garantizar tiempos de respuesta en las redes, por lo que se les denomina redes deterministicas.

"Las principales formas de manejar la memoria en las redes Token Ring son: memoria compartida, acceso directo a memoria (DMA, Direct Memory Access) y bus maestro. En lo referente a memoria compartida, una parte de la memoria de la computadora se mapea a la memoria de la tarjeta de red, lo que hace que la lectura de la tarjeta sea más rápida, debido a que la lee como si estuviera leyendo memoria RAM (Random Access Memory).

El acceso directo a memoria (DMA) ofrece una alternativa. El chip controlador de la memoria reside en la tarjeta de red y asume la responsabilidad de determinar las direcciones de origen y destino para que la información pueda ser transmitida a través del bus de datos. Desafortunadamente, la velocidad de acceso al bus de datos es de 4.77 MHz lo que provoca una degradación al momento de transmitir poca información.

El bus maestro es la mejor forma de utilizar la memoria, pero se requiere de una arquitectura de microcanal (MCA, Micro Channel Architecture), aunque también puede ser usada en la arquitectura EISA (Extended Industry Standards Architecture). La forma en que opera este tipo de tecnología es tal que el chip de la tarjeta de red controla el bus de datos, por lo que no se necesita autorización para leer o escribir en él"[7].

a) Método de Acceso

El método de acceso que utiliza esta tecnología es conocida como Token Passing, en la que una trama con ciertas características, denominada Token, es la encargada de

[7] Idem.

asignar permisos a los usuarios del anillo de una manera eficiente y garantizar de esta forma que todos los usuarios de la red tengan el mismo derecho de acceso al medio.

Existen dos premisas para evitar conflictos en el acceso a la red. La primera consiste en la necesidad de transmitir información al anillo, y la segunda, en tener la seguridad de ser los únicos transmitiendo en ese momento. La técnica utilizada para resolver este tipo de problemas se llama MAC (Media Access Control), la cual controla el medio entre los diferentes usuarios que desean tener acceso a éste para transmitir y o recibir información.

El método de acceso al medio o Token Passing trabaja de la siguiente forma:

1. El token consiste en una serie de bits únicos reconocidos por cada estación en el anillo y en la red.
2. Solamente al tener el token se puede iniciar la transmisión de la información; existe un tiempo máximo para mantener el token; una vez terminado éste, el token tiene que regresar de nuevo al anillo.
3. El token se transmite de computadora a computadora y al mismo tiempo proporciona la invitación a transmitir información. "El token siempre va a la estación siguiente según la dirección de recorrido del anillo, pero se requiere de una autorización para poder usarlo; es decir, la estación con prioridad más alta será la que transmita primero, por lo que para poder transmitir no basta con tener el token, sino que se debe tener la prioridad para hacerlo"[8].
4. Cuando la estación emisora transmite la información guarda el token y transmite una trama de datos. Dicha trama pasa de estación a estación y la información es copiada por la computadora receptora; una vez que la trama ha llegado, ésta se transmite al anillo para que termine su ciclo.
5. Después de que el destino copia la información, viaja por el anillo hasta ser leída de nuevo por la estación emisora. En el momento en que la estación emisora lee su mismo paquete libera el token al anillo para que otra estación pueda transmitir información.
6. Cada estación en el anillo regenera y repite la información en forma secuencial.
7. La adición o baja de dispositivos no interrumpe el proceso en el anillo.
8. El anillo tiene protección contra los dispositivos que tienen problemas para transmitir el token, debido a los tiempos máximos de posesión del mismo.
9. La estación que actúa como monitor activo (Active Monitor) se encarga de que todas las estaciones sigan las normas de temporización, y si alguna de las estaciones no las sigue se da de baja en la red. Además, es la encargada de purgar el anillo en el caso de existir tramas que no pertenezcan a ninguna de las estaciones y de generar el token cuando éste se haya perdido, o bien cuando la estación que tenía que mandarlo no lo hizo.

b) Codificación de Bits

La transmisión de bits sobre el anillo se hace en banda base, es decir no se emplea ninguna técnica de modulación. Debe emplearse el esquema de codificación Manchester

[8] Ídem.

diferencial para la transmisión de los bits (Figura 3.12). En este método de codificación cada bit o símbolo se codifica con una señal eléctrica formada por dos elementos de señalización de polaridad opuesta. Cada elemento de señalización asignado a un símbolo dependerá de la polaridad del segundo elemento de señalización asignado al símbolo anterior.

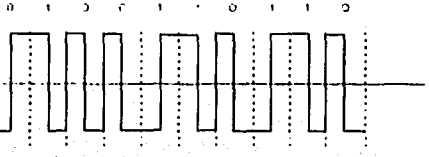


Figura 3.12: Codificación Manchester Diferencial.

La codificación de los símbolos es la siguiente:

"El 0 binario se codifica con una transición (cambio de polaridad) al inicio del intervalo del bit y con otra transición a la mitad del intervalo del bit.

El 1 binario se codifica con una transición a la mitad del intervalo del bit; es decir, el primer elemento de señalización tendrá la misma polaridad que el segundo elemento de señalización asignado al símbolo anterior"[9].

De esta forma, independientemente del símbolo codificado, siempre se tiene una transición al centro del intervalo que permite la recuperación de la señal de reloj.

Existen dos símbolos adicionales "*J*" y "*K*", los cuales se emplean en los delimitadores de las tramas y se codifican de la siguiente manera:

- Para codificar el símbolo "*J*", se transmite durante el intervalo de un bit una señal con la misma polaridad de la segunda mitad del intervalo de la señalización anterior.
- Para codificar el símbolo "*K*", se transmite durante el intervalo de un bit una señal con polaridad opuesta a la segunda mitad del intervalo de la señalización anterior: es decir, sólo hay una transición al inicio del intervalo.

En ambos casos no hay transición a la mitad del intervalo del bit, como sucede en el caso de la codificación de unos y ceros. Debido a que en la codificación Manchester diferencial siempre hay una transición en este punto; la transmisión de los símbolos "*J*" y "*K*" se considera como una violación al código. Estos símbolos son los que permiten el reconocimiento de los delimitadores de inicio y fin de la trama.

[9] Black, Uyless. 1997. Ed. AlfaOmega. "Redes de Computadoras, Protocolos, Normas e Interfaces".

c) Formato de las Tramas

A continuación se describen los campos que componen las tramas de Token Ring. (Figura 3.13).

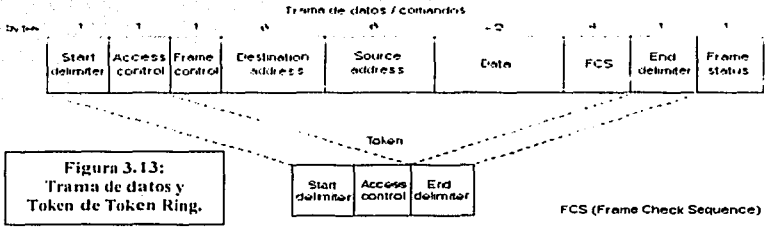


Figura 3.13: Trama de datos y Token de Token Ring.

- SD (Start Delimiter). Delimitador de Inicio. Avisa a cada una de las estaciones la llegada de un token (o trama de datos/comandos). Este campo incluye señales que distinguen el byte del resto de la trama, violando el esquema de codificación que se utiliza en las demás partes de la misma. Este byte está formado por la secuencia de símbolos jk0jk000.

- AC (Access Control). Control de Acceso. Contiene el campo ***Prioridad*** (los tres bits más significativos) y el campo ***Reservación*** (los 3 bits menos significativos), así como un bit de ***Token*** (que se utiliza para diferenciar un token de una trama de datos/comandos) y un bit de ***Supervisión*** (que utiliza el supervisor activo para determinar si una trama está circulando indefinidamente por el anillo). Este byte está formado por los bits PPPTSRRR

1. Bits PPP. Estos tres bits indican la prioridad del token o de la trama. Para poder enviar información es necesario tener disponible el token y que la prioridad de la estación sea mayor o igual a la prioridad del token.
2. Bit T. Tiene un valor de 0 en caso de tratarse de un token. Cuando una computadora desea enviar información, espera un token con prioridad menor o igual a la prioridad de la trama a transmitir y cambia el valor del bit a 1. Con esto se forma una secuencia de inicio de trama de forma tal que el token ya no se encuentra disponible para otras estaciones en el anillo.
3. Bit S. Este bit se transmite con un valor de 0. Cuando el monitor activo (Active Monitor) lo retransmite le cambia el valor a 1. También ayuda en la detección y corrección de situaciones en las que un token o trama con alta prioridad circulan indefinidamente.
4. Bits RRR. En estos bits una estación puede reservar la prioridad del token siguiente.

- FC (Frame Control), Control de Trama. Indica si la trama contiene datos o información de control. En las tramas de control este byte se utiliza para especificar el tipo información. Está formado por los bits FFZZZZZZ. Los bits

FF indican el tipo de trama (MAC o LLC). Los bits ZZZZZZ indican el subtipo de una trama MAC (son bits de control).

- DA (Destination Address). Dirección Destino. Este campo puede tener una longitud de dos a seis bytes. Todas las direcciones de la red deben tener la misma longitud. El bit **I/G** indica si se trata de una dirección individual o de grupo; mientras que el bit **U/L** indica si se trata de una dirección administrada universal o localmente (para el caso de direcciones universales se consideran los 6 bytes).

- SA (Source Address). Dirección Fuente. El formato y la longitud de este campo deben ser iguales a los del campo DA y el bit I/G debe ser igual a 0.

- Data (Información). Contiene información destinada a las capas MAC o LLC. La longitud de este campo está limitada por el tiempo de conservación del token en el anillo, que define el tiempo máximo que una estación puede conservar el token en su poder: el tiempo de transmisión no debe ser mayor al tiempo de posesión del token.

- FCS (Frame Check Sequence). Secuencia de Verificación de Trama. Estos 4 bytes contienen información para detectar errores en la transmisión; este campo es llenado por la estación origen con un valor calculado en función del contenido de la trama (a partir de los campos FC, DA, SA y Data). La estación destino recalcula este valor para determinar si se dañó la trama en su tránsito por el anillo; si es el caso, dicha trama es eliminada.

- ED (End Delimiter). Delimitador de Final. Este campo indica el final de un token o una trama de datos/comandos. También contiene bits para señalar una trama dañada e identifica la trama ubicada al final de una secuencia lógica. Este byte está formado por la secuencia de símbolos jk1jk1IE

1. Bit I. Puede usarse para determinar el fin de la transmisión de una estación. Para la transmisión de una serie de tramas, el bit I toma el valor de 1 en la primera trama y en las tramas intermedias. El bit I cambia a 0 en caso de que se transmita una sola trama o cuando se transmite la última trama de una secuencia.
2. Bit E. Este bit se transmite con un valor de 0. Todas las estaciones del anillo analizan las tramas y los tokens que pasan a través de ellas y repiten este bit con el valor que reciben, excepto cuando detectan un error, en cuyo caso este bit adquiere un valor de 1.

- FS (Frame Status), Estado de la Trama. Este byte se utiliza para terminar una trama de datos/comandos; incluye el indicador de confirmación de dirección y el indicador de copiado de la trama. Está formado por los bits DCrrDCrr y ayuda a la estación transmisora a detectar las siguientes condiciones:

1. La estación de destino no existe o no está activa.
2. La estación de destino existe, pero no copió la trama.

3. La trama fue copiada.

Para esto, los bits D y C se transmiten con el valor de 0. Si la estación de destino existe y reconoce su dirección en el campo DA de la trama, entonces cambia el valor de los bits D a 1. Si la estación copia la trama, cambia el valor de los bits C a 1.

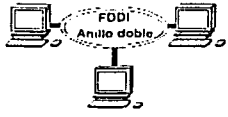
3.2.3. FDDI (Fiber Distributed Data Interface)

La necesidad de transmitir a mayores velocidades surgió debido a los requerimientos de transmisión de aplicaciones gráficas y de video, las cuales necesitan enviar millones de bits en tiempos muy cortos, lo que obliga a tener redes de alta velocidad como lo son las redes FDDI que transmiten a 100 Mbps.

El proceso de estandarización comenzó en 1982 y logró su estabilidad a finales de los años 80's. FDDI utiliza una tecnología de token y fue desarrollada para poder soportar la interconexión con las redes de área local, aunque en sus inicios se consideraba el uso de esta tecnología solamente para el backbone en edificios o campus. En la actualidad, esta tecnología se utiliza como una alternativa en las redes de área local.

Las redes FDDI se componen de un anillo doble de fibra óptica por paso de testigo, el cual ayuda a mantener un nivel de tolerancia a fallas en el caso de que se presenten en alguna parte de la red (Figura 3.14). El paso de testigo "token-ring" se refiere al método por el que un nodo conectado al anillo FDDI accesa a él. La topología en anillo se implanta físicamente con fibra óptica. Uno de los anillos es el encargado de transmitir datos, mientras que el otro se utiliza para transmitir tramas de control.

Figura 3.14: Red FDDI.



a) Componentes Básicos de las Redes FDDI

Los nodos no pueden transmitir datos hasta que toman el token. Cuando un nodo detecta esta trama y tiene datos que transmitir, captura la trama eliminándola del anillo, y la libera cuando termina o cuando finaliza su tiempo de posesión del token. El cable duplex de fibra óptica consiste en dos cables idénticos, que implantan en realidad dos anillos con sentidos de rotación opuestos.

Los estándares definen los componentes de las redes que se deben incluir y son: SAS (Single Attachment Station), DAS (Dual Attachment Station) y sus respectivos conectores. Las estaciones que usan SAS están conectadas a un concentrador con topología física de estrella, cuyas características principales son:

1. La falla de una de las estaciones, tanto en cableado como en hardware, no afecta el funcionamiento de la red, pero desconectará totalmente al nodo de la red.
2. En la configuración SAS la falla en el concentrador provoca que la red entera deje de funcionar.
3. Las estaciones conectadas en DAS, por lo general forman una topología de anillo y todas las estaciones están conectadas a ambos anillos, el primario y el secundario (Figura 3.15).

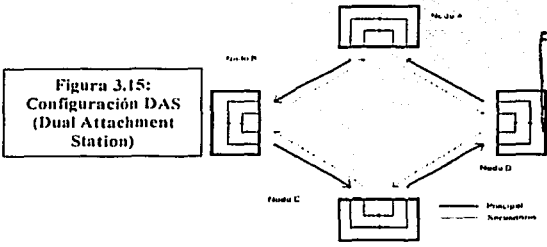


Figura 3.15: Configuración DAS (Dual Attachment Station)

"Las redes FDDI pueden alcanzar distancias entre 3 y 40 km dependiendo del tipo de fibra que se emplee. El método de acceso al medio utilizado es Token Passing: en este tipo de tecnología se pueden tener múltiples tramas al mismo tiempo en el anillo sin que tengan que ser reconocidas por sus destinatarios, además se utiliza transferencia de información asíncrona, lo que genera una mayor velocidad de transferencia"[10].

b) Formato de las Tramas

"La trama de FDDI tiene un tamaño máximo de 4500 bytes, lo que es ideal para transferir grandes volúmenes de información. El campo de "preamble" contiene una secuencia de unos para sincronizar la trama con los relojes de todas las estaciones en el anillo o estrella; enseguida del preámbulo se encuentra el campo SD, que es donde comienza la trama; después sigue el campo de FC, que indica si la transmisión se llevará a cabo en modo síncrono o asíncrono, si usará un direccionamiento de 16 o de 48 bits y si el tipo de trama que se enviará será MAC o LLC; el resto de los campos son parecidos a los utilizados en la trama de Token Ring"[11] (Figura 3.16).

- Preamble (Preámbulo). Es una secuencia única que prepara a cada estación para recibir una trama entrante. Sincroniza la trama con el reloj de cada estación. El emisor de la trama envía el campo con 16 bits I (Idle), los nodos que repiten la trama alrededor del anillo pueden cambiar la longitud de este campo de acuerdo con sus requerimientos de sincronización.

[10] Rodríguez, G. y E., Jorge. 1996. Ed. McGraw-Hill. "Introducción a las Redes de Área Local".
[11] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".

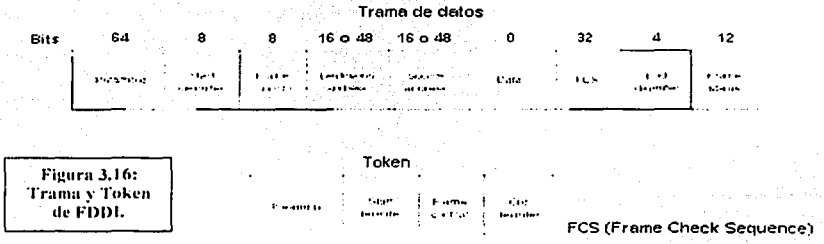


Figura 3.16: Trama y Token de FDDI.

- SD (Start Delimiter), Delimitador de Inicio. Indica el comienzo de la trama a través de un patrón de señalización que lo diferencia del resto de la trama. Consta de un símbolo *j*, seguido de un símbolo *k*.

- FC (Frame Control), Control de Trama. Indica el tipo de la trama. Este campo está constituido por los bits CLFFZZZZ. El bit C especifica la clase de trama (síncrona o asíncrona); el bit L indica si la longitud de los campos de direcciones es de 16 o de 48 bits, los bits FF indican si la trama contiene información del usuario (LLC) o información de control (MAC) y los bits ZZZZ especifican la prioridad de la trama LLC o el tipo de trama MAC.

- DA (Destination Address), Dirección Destino. Especifica la dirección de la máquina a la cual va dirigida la trama; puede ser una dirección de unicast (única), de multicast (grupo) o de broadcast (todas las máquinas). En una misma red pueden coexistir estaciones con direcciones de 16 bits y estaciones con direcciones de 48 bits.

- SA (Source Address), Dirección Origen. Especifica la dirección de la máquina que envío la trama.

- Data (Información). Contiene los datos del usuario o información de control MAC; la longitud máxima de trama es de 4500 bytes, sin incluir los bytes del campo preamble.

- FCS (Frame Check Sequence), Secuencia de Verificación de Trama. Este campo de 4 bytes sirve para detectar si hubo errores durante la transmisión de la trama. Este campo es llenado por la estación origen con el valor de la verificación de redundancia cíclica que se calcula en función del contenido de la trama (campos FC, DA, SA y Data). La máquina destino recalcula el valor para determinar si la trama se dañó en su tránsito por la red; si es el caso, dicha trama es eliminada.

- ED (End Delimiter), Delimitador de Final. Este campo contiene campos, que no pueden ser datos, y que indican el final de la trama. Consta de un símbolo T (dos si se trata de un token) e indica el final de la trama. Como el símbolo T no forma

parte de los 16 símbolos de datos, el campo ED no puede confundirse con símbolos de otros campos de la trama.

- FS (Frame Status). Estado de la Trama. Permite que la estación origen determine si se ha presentado un error o si la trama fue copiada y confirmada por una estación receptora. "Contiene tres indicadores: E (Error), A (Address, Dirección) y C (Copy, Copiado). Cuando la estación emisora transmite una trama coloca en el campo FS tres símbolos R (Reset). Al circular la trama por la red, si una estación detecta un error en la transmisión coloca en el indicador E el símbolo S (Set); si una estación detecta su dirección en el campo DA, cambia a S el indicador A y si además copia la trama, cambia el indicador C a S. Los indicadores A y C permiten que la estación emisora determine, al regresar su trama, el estado de la estación receptora: si no existe o no está activa, si existe pero no copió la trama o si existe y copió la trama"[12].

c) Aplicaciones

FDDI proporciona interconexión a alta velocidad entre redes LAN, y entre éstas y las redes WAN. Las principales aplicaciones se han centrado en la interconexión de redes LAN Ethernet y de éstas con redes WAN X.25. Tanto en la conexión de estas tecnologías de red como con otras, todas se conectan directamente a la red principal FDDI (backbone). Otra aplicación es la interconexión de periféricos remotos de alta velocidad a computadoras tipo mainframe.

Para garantizar el funcionamiento, cuando una máquina está desconectada, averiada o apagada, un conmutador óptico de funcionamiento mecánico realiza un puenteo del nodo, eliminándolo del anillo. Esta seguridad, unida al hecho de la compatibilidad entre velocidades de 100 Mbps con distancias de 100 Km hacen de FDDI una tecnología óptima para gran número de aplicaciones.

3.3. Tecnologías WAN (World Area Network)

3.3.1. HDLC (High-Level Data Link Control)

El protocolo más importante para el enlace de datos es HDLC (ISO 3309, ISO 4335), no solo porque es el más utilizado, sino porque además es la base para otros protocolos importantes de la capa de enlace de datos, en los que se usan formatos similares y procedimientos iguales a los que se usan en HDLC.

a) Características Básicas

Para satisfacer las demandas de un buen número de aplicaciones, HDLC define tres tipos de estaciones, dos configuraciones del enlace y tres modos de operación para la transferencia de los datos, los tres tipos de estaciones son:

[12] Rodríguez, G. y E., Jorge. 1996. Ed. McGraw-Hill. "Introducción a las Redes de Área Local".

- Estación Primaria. Tiene la responsabilidad de controlar el funcionamiento del enlace, las tramas generadas por la primaria se denominan órdenes.
- Estación Secundaria. Funciona bajo el control de la estación primaria, las tramas generadas por la estación secundaria se denominan respuestas; la primaria establece un enlace lógico independiente para cada una de las secundarias presentes en la línea.
- Estación combinada. Es una mezcla entre las características de las primarias y las secundarias; una estación de este tipo puede generar tanto órdenes como respuestas.

Las dos posibles configuraciones del enlace son:

- Configuración no balanceada. Está formada por una estación primaria y una o más secundarias, permite tanto transmisión full-duplex como half-duplex.
- Configuración balanceada. Consiste en dos estaciones combinadas, permite igualmente transmisión full-duplex o half-duplex.

Los tres modos de transferencia de datos son:

- NRM (Normal Response Mode). Modo de Respuesta Normal. Se utiliza en la configuración no balanceada. La estación primaria puede iniciar la transferencia de datos a la secundaria, pero la secundaria solo puede transmitir datos usando respuestas a las órdenes emitidas por la primaria.
- ABM (Asynchronous Balanced Mode). Modo Balanceado Asíncrono. Se utiliza en la configuración balanceada; en este modo cualquier estación combinada podrá iniciar la transmisión sin necesidad de recibir permiso por parte de la otra estación combinada.
- ARM (Asynchronous Response Mode). Modo de Respuesta Asíncrono. Se utiliza en la configuración no balanceada; la estación secundaria puede iniciar la transmisión sin tener permiso explícito por parte de la primaria. La estación primaria sigue teniendo la responsabilidad del funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores y la desconexión lógica.

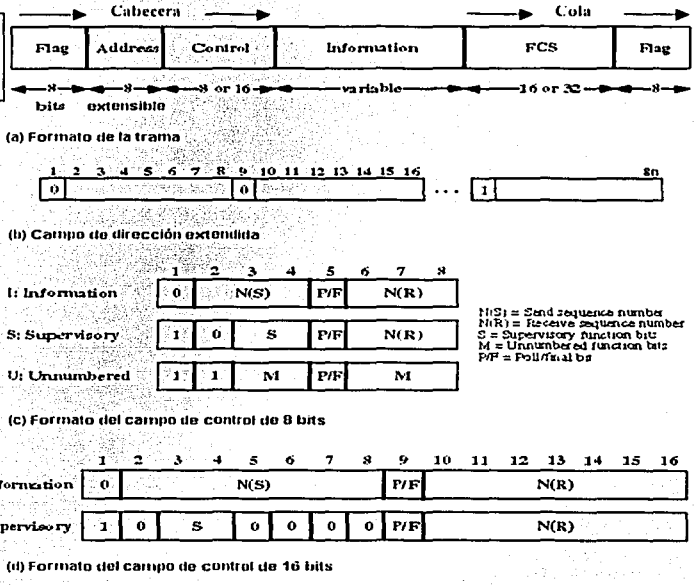
"El NRM se usa en líneas que tienen múltiples conexiones, en las que varias terminales se conectan a una computadora central. La computadora sondea cada una de las entradas correspondientes a las distintas terminales. El NRM se usa en ocasiones para los enlaces punto a punto, especialmente si el enlace conecta una terminal u otros dispositivos periféricos a la computadora. El ABM es el más utilizado de los tres modos; debido a que en ABM no se necesita hacer sondeos la utilización de los enlaces punto a punto con full-duplex es más eficiente. ARM no se utiliza tan frecuentemente; es útil en algunas situaciones particulares en las que la estación secundaria necesita iniciar la transmisión"[13].

[13] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

b) Estructura de la Trama

HDLC utiliza transmisión síncrona, todos los intercambios se realizan a través de tramas. HDLC utiliza un formato único de tramas que es válido para todos los intercambios posibles: datos e información de control.

Figura 3.17: Estructura de la trama HDLC.



A los campos Flag, Address y Control, que preceden al campo de Information se les denomina cabecera. El FCS junto con el otro campo de Flag que están a continuación del campo Information se les denomina cola (Figura 3.17).

- Flag (Bandera o Delimitador). Los campos de delimitación están localizados en los dos extremos de la trama y ambos corresponden a la siguiente combinación de bits 01111110, se puede usar un delimitador único como final y comienzo de la siguiente trama simultáneamente; a ambos lados de la interfaz entre el usuario y la red, los receptores estarán continuamente intentando detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama. Cuando se recibe una trama, la estación seguirá intentando detectar esa misma secuencia para determinar el final de la trama.

Debido a que el protocolo permite cualquier combinación de bits (es decir, no existe ninguna restricción en el contenido de los campos) no hay garantía de que la combinación 01111110 no aparezca en algún lugar dentro de la trama, destruyendo así la sincronización. Para evitar esta situación no deseable, se realiza un procedimiento denominado inserción de bits. "En la transmisión de los bits que están entre los dos delimitadores de comienzo y final, el transmisor insertará un 0 extra siempre que se encuentre con la aparición de cinco 1 consecutivos. El receptor, después de haber detectado el delimitador de comienzo, monitorea la cadena de bits recibida, de tal manera que cuando aparezca una combinación de cinco 1 seguidos, el sexto bit será examinado; si dicho bit es 0, se eliminará sin más, pero si es 1 y el séptimo bit es 0, la combinación se considera como un delimitador. Si los bits sexto y séptimo son iguales a 1 se interpreta como una indicación de cierre generada por el emisor"[14].

Al usar el procedimiento de inserción de bits, el campo de datos puede contener cualquier combinación arbitraria de bits, esta propiedad se denomina transparencia en los datos.

- Address (Dirección). El campo de dirección identifica a la estación secundaria que ha transmitido o que va a recibir la trama, este campo no se necesita en enlaces punto a punto, pero se incluye por cuestiones de uniformidad. "El campo de dirección tiene normalmente 8 bits, sin embargo tras una negociación previa, se puede utilizar un formato ampliado en el que la dirección tendrá un múltiplo de 7 bits. El bit menos significativo de cada octeto será respectivamente 1 o 0, si es o no el último octeto del campo de dirección. Los 7 bits restantes en cada octeto formarán una dirección propiamente dicha, un octeto de la forma 11111111 se interpretará como una dirección que corresponde a todas las direcciones, tanto en el formato básico como el ampliado"[15]: este tipo de direccionamiento se utiliza cuando la estación primaria requiere enviar una trama a todas las secundarias.

- Control. En HDLC existen tres tipos de tramas, cada una de ellas con un formato diferente para el campo de control. Las *tramas de Information - Información* - (Tramas I) transportan los datos generados por el usuario; además se incluye información para el control ARQ (Automatic Repeat Request) de errores y del flujo. Las *tramas de Supervisory - Supervisión* - (Tramas S) proporcionan el mecanismo ARQ cuando la incorporación de las confirmaciones en las tramas de información no es factible. Las *tramas Unnumbered - No Numeradas* - (Tramas U) proporcionan funciones complementarias para controlar el enlace. El primer o los dos primeros bits del campo de control se utilizan para identificar el tipo de trama, los bits restantes se estructuran en subcampos (Figura 3.17 c y d).

Todos los formatos posibles del campo de control contienen el bit P/F (Poll/Final), su utilización es dependiente del contexto, normalmente en las tramas de órdenes se

[14] Idem.
[15] Idem.

denomina bit P y se fija a 1 para solicitar una respuesta a la entidad HDLC par. En las tramas de respuesta, el bit se denomina F y su valor se fija a 1 para identificar a la trama el tipo de respuesta devuelta tras la recepción de una orden.

"El campo de control básico en las tramas S y en las tramas I utiliza números de secuencia de tres bits; utilizando una orden que fije un modo adecuado en estas tramas, se puede hacer uso de un campo de control ampliado en el que los números de secuencia sean de 7 bits. Las tramas U siempre tienen un campo de control de 8 bits"[16].

- Information (Información). El campo de información solo está presente en las tramas I y en algunas tramas U, este campo puede contener cualquier secuencia de bits, con la única restricción que el número de bits sea igual a un entero múltiplo de 8; la longitud del campo de información es variable y siempre será menor que un valor máximo predefinido.

- FCS (Frame Check Sequence). Secuencia de Comprobación de Trama. El contenido del campo FCS es un código para la detección de errores calculado a partir de los bits de la trama excluyendo los delimitadores, el código que se usa normalmente es el CRC-CCITT (Cyclic Redundancy Check – International Consultative Committee on Telegraphy and Telephony) de 16 bits.

c) Funcionamiento

El funcionamiento de HDLC consiste en el intercambio de tramas I, tramas S y tramas U entre dos estaciones. En la tabla 3.1 se definen las órdenes y respuestas posibles para los distintos tipos de tramas.

Tabla 3.1. Órdenes y respuestas del protocolo HDLC.

Nombre	Órdenes / Respuestas	Descripción
Information (I)	O/R	Intercambio de datos de usuario.
Supervisory (S)		
Receive Ready (RR)	O/R	Confirmación positiva; preparado para recibir tramas I.
Receive Not Ready (RNR)	O/R	Confirmación negativa; no preparado para recibir.
Reject (REJ).	O/R	Confirmación negativa; adelante-atrás-N.
Selective Reject (SREJ)	O/R	Confirmación negativa; rechazo selectivo.
Unnumbered (U)		
Set Normal Response Mode / Set Normal Response Mode Extended (SNRM / SNRME).	O	Fija el modo; extendido = números de secuencia de 7 bits.
Set Asynchronous Response Mode / Set Asynchronous Response Mode Extended (SARM / SARME).	O	Fija el modo; extendido = números de secuencia de 7 bits.
Set Asynchronous Balanced Mode /	O	Fija el modo; extendido = números de

[16] Ídem.

Set Asynchronous Balanced Mode Extended (SABM / SABME).		secuencia de 7 bits.
Set Initialization Mode (SIM).	O	Inicia las funciones de control del enlace en la estación direccionada.
Disconnect (DISC).	O	Finaliza la conexión lógica del enlace.
Unnumbered Acknowledged (UA).	R	Confirma la aceptación de una de las órdenes para fijar el modo.
Disconnected Mode (DM).	R	Finaliza la conexión lógica del enlace.
Request Disconnect (RD).	R	Solicitud de una orden DISC.
Request Initialization Mode (RIM).	R	Se necesita iniciación; solicitud de la orden SIM.
Unnumbered Information (UI).	O/R	Se utiliza para intercambiar información de control.
Unnumbered Poll (UP).	O	Se utiliza para intercambiar información de control.
Reset (RSET).	O	Se utiliza para as recuperaciones; pone N(R) y N(S) a sus valores iniciales.
Exchange Identification (XID).	O/R	Se utiliza para solicitar o informar sobre el estado.
Test (TEST).	O/R	Intercambio de campos idénticos de información para test.
Frame Reject (FRMR).	R	Informa sobre la recepción de una trama inaceptable.

El funcionamiento de HDLC implica 3 fases. Primero. Uno de los dos extremos inicia el enlace de datos, de tal manera que las tramas se puedan intercambiar de una forma ordenada, durante esta fase se pactan las opciones que se usarán en el intercambio posterior. Después de la iniciación los dos extremos intercambian los datos generados por los usuarios, así como información de control para llevar a cabo los procedimientos de control del flujo y de errores. Finalmente uno de los dos extremos comunicará la finalización de la transmisión.

1. Iniciación

La iniciación la puede solicitar cualquiera de los dos extremos transmitiendo una de las seis órdenes previstas para fijar el modo; esta orden sirve para tres cosas:

- Avisar al otro extremo sobre la solicitud de la iniciación.
- Especificar cuál de los tres modos (NRM, ABM, ARM) se está solicitando.
- Especificar si se van a utilizar números de secuencia de 3 o 7 bits.

Si el otro extremo acepta la solicitud, se informará al extremo sobre esta contingencia mediante la transmisión de una trama de confirmación no numerada (UA, Unnumbered Acknowledged). Si la solicitud se rechaza, se envía una trama de modo desconectado (DM, Disconnected Mode).

2. Transferencia de Datos

Una vez que ha sido aceptada la solicitud de iniciación se establece la conexión lógica, a partir de entonces ambos lados pueden comenzar a enviar datos a través de tramas I, comenzando con el número de secuencia 0. Los campos N(S) y N(R) de una trama I contendrán los números de secuencia con los que se lleva a cabo el control de flujo y de errores. "La secuencia de tramas I se numerará consecutivamente módulo 8 o módulo 128, dependiendo de si se utilizan 3 o 7 bits respectivamente, utilizando el campo N(S). El campo N(R) se utiliza para la confirmación de las tramas I recibidas, facilitando de esta forma que el modulo HDLC indique al otro extremo el número de trama I que se espera recibir"[17].

Las tramas S también se utilizan para controlar el flujo y los errores. La trama receptor preparado (RR, Receive Ready) confirma la recepción de una trama I, indicando a su vez, la siguiente trama I que se espera recibir. La RR se usa cuando no hay tráfico en el sentido contrario (Tramas I) en el que se pueden incluir las confirmaciones. La trama receptor no preparado (RNR, Receive Not Ready) confirma la recepcion de una trama I como lo hace la RR, pero a la vez solicita a la entidad ubicada en el otro extremo del enlace que suspenda la transmisión de las tramas I. Cuando la entidad que envio la trama RNR esté preparada de nuevo, enviará una RR. La trama REJ (Reject) sirve para iniciar el procedimiento ARQ go-back-N (ARQ con vuelta-atrás-N), con lo que se indica que la última trama I recibida se ha rechazado y solicita la retransmision de todas las tramas I con números de secuencia posteriores a la N(R). La trama de rechazo selectivo (SREJ, Selective Reject) se usa para solicitar la retransmisión de una sola trama.

3. Desconexión

Cualquiera de las dos entidades situadas a ambos extremos del enlace puede iniciar la desconexión, tanto por iniciativa propia (si es que ha habido algún tipo de falla) como por una solicitud de las capas superiores. HDLC lleva a cabo la desconexión transmitiendo una trama de desconexión (DISC, Disconnect). El otro extremo podrá aceptar dicha desconexión devolviendo una trama UA e informando al usuario de la capa 3 sobre el cierre de la conexión.

3.3.2. Frame Relay

a) Antecedentes

Frame Relay es un protocolo WAN de alto desempeño que opera en la capa física y de enlace de datos del modelo de referencia OSI. Es un ejemplo de la tecnología de conmutación de paquetes, en donde las estaciones terminales comparten el medio de transmisión de la red de manera dinámica, así como el ancho de banda disponible. Los paquetes de longitud variable se utilizan en transferencias más eficientes y flexibles; posteriormente estos paquetes se conmutan entre los diferentes segmentos de la red hasta que llegan a su destino. Las técnicas de multiplexaje estadístico controlan el acceso a la red

[17] Ídem.

en un entorno de conmutación de paquetes; la ventaja de esta técnica es que permite un uso más flexible y eficiente del ancho de banda.

"Frame Relay es estrictamente una arquitectura de protocolos de la capa 2 (capa de enlace) del modelo OSI, en tanto que X.25 también proporciona servicios de la capa 3 (capa de red), debido a esta situación Frame Relay supera en desempeño y eficiencia en la transmisión a X.25, y a su vez resulta más apropiado para las aplicaciones WAN actuales como la interconexión con redes LAN" [18].

b) Estandarización de Frame Relay

La propuesta inicial para la estandarización de Frame Relay se presentó al CCITT en 1984, sin embargo, por su falta de interoperabilidad y estandarización no tuvo gran aceptación a finales de los años 80.

En 1990 ocurrió un gran desarrollo en la historia de Frame Relay cuando las compañías Cisco, Northern Telecom, Digital Equipment, Stratacom y Convex Computer formaron un consorcio para aplicarse al desarrollo de la tecnología Frame Relay. Dicho consorcio desarrolló una especificación que conformó el protocolo básico de Frame Relay que se estaba analizando en el CCITT, pero ampliaba el protocolo con características que ofrecían facilidades adicionales en entornos complejos e interconectividad de redes.

"El primer servicio público basado en Frame Relay apareció en Estados Unidos en 1992 bajo los auspicios de AT&T y BT North America. Los primeros nodos se situaron en las ciudades más importantes de forma que sus habitantes podían accesar al servicio de forma directa; para los usuarios situados en el resto de las ciudades el acceso al servicio de los nodos se proporcionaba mediante unos puntos de presencia (lugares físicos donde un portador de larga distancia sitúa la interfaz con un LEC – Local Exchange Carrier –) facilitado por las compañías telefónicas locales"[19].

Hoy en día Frame Relay se define como un estándar del CCITT y del ANSI que define un proceso para el envío de datos a través de una red de datos pública o privada. Es una tecnología eficiente de conmutación rápida de paquetes de datos, llamados tramas, de alto desempeño que puede utilizarse como un protocolo de transporte y acceso en redes públicas o privadas de todo el mundo, a fin de brindar servicios de telecomunicaciones. Frame Relay es una forma de enviar información a través de una WAN dividiendo los datos en paquetes. Cada paquete viaja a través de una serie de switches en una red Frame Relay para alcanzar su destino. Ha sido especialmente adaptado para velocidades de hasta 2 Mbps, aunque nada le impide superarlas.

Opera en la capa física y de enlace de datos del modelo de referencia OSI, pero depende de los protocolos de las capas superiores como TCP para la corrección de errores. Actualmente Frame Relay es un protocolo de capa de enlace de datos conmutado de

[18] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".
[19] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Segundo Año".

estándar industrial que maneja múltiples circuitos virtuales mediante el encapsulamiento de HDLC entre los dispositivos conectados.

c) Dispositivos Frame Relay

Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales: DTE (Data Terminal Equipment) y DCE (Data Circuit-terminating Equipment) (Figura 3.18). Los DTE's, en general, se consideran como equipo terminal para una red específica y se localizan, regularmente, en las instalaciones del cliente: de hecho, pueden ser propiedad del cliente. Algunos ejemplos de dispositivos DTE son las terminales, computadoras personales, ruteadores y bridges.

Los DCE son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia: su propósito es proporcionar los servicios de temporización y conmutación en una red: son en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos son switches de paquetes.

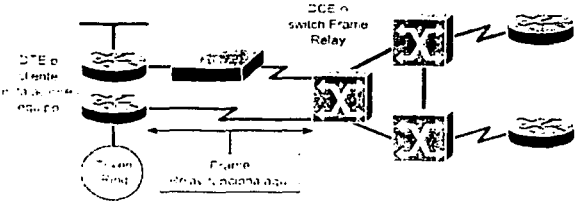


Figura 3.18: Red con tecnología Frame Relay.

La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas, funcionales y de procedimiento para la conexión entre dispositivos. Una de las especificaciones de la interfaz de la capa física que más se utiliza es RS-233 (Recommended Standard 232). El componente de la capa de enlace de datos define el protocolo que establece la conexión entre el dispositivo DTE que puede ser un ruteador, y el dispositivo DCE que puede ser un switch.

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una sola trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Este equipo se denomina FRAD (Frame Relay Assembler/Disassembler) y el nodo de red se denomina FRND (Frame Relay Network Device).

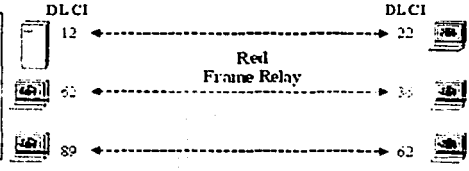
d) Circuitos Virtuales

Frame Relay ofrece comunicación de la capa de enlace de datos orientada a conexión, lo que significa que hay una comunicación definida entre cada par de

dispositivos y que estas conexiones están asociadas con un identificador de conexión. Este servicio se implanta por medio de Circuitos Virtuales (Virtual Circuit - VC -). Un Circuito Virtual son dos vías, definidas por software, de una trayectoria entre dos puertos que actúa como una línea privada en la red: es una conexión lógica creada entre dos DTE a través de una red de conmutación de paquetes.

Los circuitos virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifican de manera única a través de los DLCI's. "Un DLCI es un número que identifica el extremo final en una red Frame Relay, normalmente estos valores son asignados por el proveedor del servicio Frame Relay (en su caso, la compañía telefónica). Los DLCI's Frame Relay tienen un significado local, lo que quiere decir que los valores en sí mismos no son únicos en la WAN Frame Relay"[20]; por ejemplo, dos dispositivos DTE conectados a través de un circuito virtual, pueden usar un valor diferente de DLCI para hacer referencia a la misma conexión (Figura 3.19). Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (switches) ubicados en la red de conmutación de paquetes Frame Relay.

Figura 3.19: Uso de circuitos virtuales con DLCI's diferentes en Frame Relay.



Existen dos tipos de conexiones virtuales Frame Relay: PVC (Permanent Virtual Circuit) y SVC (Switched Virtual Circuit). En un principio los PVC's fueron los primeros servicios ofrecidos, pero los productos y servicios SVC están creciendo en popularidad.

1. SVC (Switched Virtual Circuit)

Los SVC's son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una transferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de 4 estados:

- Establecimiento de la llamada. Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
- Transferencia de datos. Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- Ocioso. La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.

[20] Ídem.

- Terminación de la llamada. Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual, los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Hoy en día pocos fabricantes de equipo DCE Frame Relay soportan SVC's; por lo tanto su utilización real es mínima en las redes Frame Relay existentes.

2. PVC (Permanent Virtual Circuit)

Los estándares Frame Relay direccionan circuitos virtuales permanentes (PVC) que se encuentran administrativamente configurados y administrados en una red Frame Relay. Los PVC de Frame Relay son identificados por los DLCI (Figura 3.20).

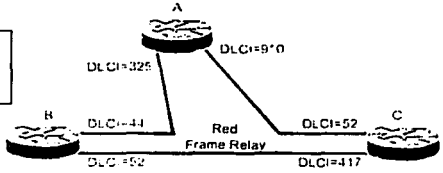


Figura 3.20: PVC's asociados a su respectivo DCI.

Los PVC's son conexiones establecidas en forma permanente que se utilizan en transferencias de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La trayectoria en cuestión toma a través de la red varias formas de tiempo en tiempo, lo que significa que el redireccionamiento automático del circuito cambia sin afectar el comienzo y el final del mismo. En este sentido se puede decir que un PVC es similar a un circuito dedicado punto a punto. La comunicación a través de un PVC no requiere los estados de establecimiento y finalización de la llamada que se utilizan en los SVC's. Los PVC's siempre operan en alguno de los siguientes estados:

- Transferencia de datos. Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- Ocioso. Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVC's, los PVC's no se darán por finalizados en ninguna circunstancia.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

3. Parámetros de Dimensionamiento del PVC

- Velocidad de acceso. La velocidad medida por reloj (velocidad de puerto) de la conexión (loop local) a la nube Frame Relay. Es equivalente a la velocidad a la que los datos viajan hacia dentro o fuera de la red.

- CIR (Committed Information Rate). Taza de Información Suscrita. Es la velocidad garantizada, en bits por segundo, que el proveedor del servicio se compromete a proporcionar. Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cada sentido (Figura 3.21, Tramas 1 y 2).
- Bc (Committed Burst Size). Ráfaga Suscrita. Cantidad máxima de bits que el switch acepta transferir durante un intervalo de tiempo. Es la cantidad de bits transmitidos en el periodo T a la tasa CIR (CIR=Bc/T). En las redes Frame Relay se permite al usuario enviar picos de tráfico a la red por encima del CIR, durante intervalos de tiempo muy pequeños, incluidos en el periodo T.
- Be (Excess Burst Size). Ráfaga Excesiva. Cantidad máxima de bits no suscritos que el switch Frame Relay intenta transferir más allá del CIR. La ráfaga excesiva depende de las ofertas de servicio que el distribuidor coloca a disposición, pero se limita generalmente a la velocidad de puerto del loop de acceso local. Es la cantidad de bits transmitidos en el periodo T por encima de la tasa CIR. Si la red tiene capacidad libre suficiente admitirá la entrada de este tipo de tráfico en exceso (Figura 3.21, Trama 3), marcándolo con el bit DE activo.

El tráfico entrante en la red, por encima de Bc + Be, es el descartado directamente en el nodo de entrada (Figura 3.21, Trama 4).

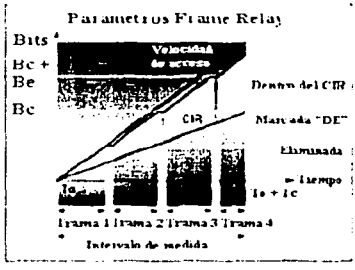


Figura 3.21: Parámetros de dimensionamiento de los PVC's.

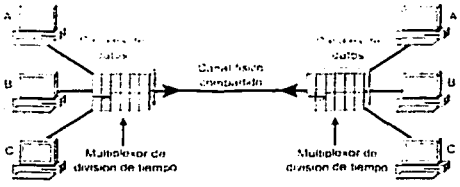
4. Multiplexaje en Frame Relay

Como interfaz entre el equipo del usuario y de red Frame Relay proporciona un medio para realizar el multiplexaje de varias conversaciones de datos lógicos, denominadas circuitos virtuales, a través de un medio físico compartido asignando un DLCI a cada par de dispositivos DTE/DCE (Figura 3.22).

El multiplexaje Frame Relay permite un uso más flexible y eficiente del ancho de banda disponible. Por lo tanto, Frame Relay permite a los usuarios compartir el ancho de banda a un costo reducido. Por ejemplo, supongamos que se tiene una WAN que utiliza Frame Relay y que Frame Relay es equivalente a un grupo de rutas. La compañía telefónica generalmente es propietaria de las rutas y está a cargo de su mantenimiento. Se puede elegir

arrendar la ruta exclusivamente para una empresa (dedicada), o bien se puede pagar menos para arrendar una ruta compartiéndola con otras empresas. Por supuesto, Frame Relay también se puede ejecutar totalmente en redes privadas; sin embargo, rara vez se utiliza de esta manera.

Figura 3.22: Multiplexaje en Frame Relay.



Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red; a menudo esta característica permite conectar múltiples dispositivos DTE con menos equipo y mantener una red menos compleja.

Frame Relay proporciona un medio para realizar el multiplexaje de varias conversaciones de datos lógicos. El equipo de conmutación del proveedor de servicios genera una tabla asignando los valores DLCI a puertos salientes. Cuando se recibe la trama, el dispositivo de conmutación analiza el identificador de conexión y entrega la trama al puerto saliente asociado. La ruta completa al destino se establece antes de enviar la primera trama.

e) Principios de Frame Relay

El protocolo Frame Relay se basa en los siguientes principios:

- El medio de transmisión y las líneas de acceso están prácticamente libres de errores.
- La corrección de errores se proporciona por los niveles superiores de los protocolos de las aplicaciones de usuario.
- La red, en estado normal de operación, no está congestionada y existen mecanismos estándares de prevención y tratamiento de la congestión.

El primer principio básico señala que muchos de los protocolos más antiguos, tales como X.25, se diseñaron para operar mediante circuitos analógicos con errores. Esto exigía al protocolo de comunicaciones el uso de procedimientos complejos de control de errores y confirmación de información transmitida y recibida correctamente. Con la aparición de líneas de transmisión digitales, se redujo considerablemente la necesidad de estos procedimientos.

Como consecuencia en el segundo principio básico de Frame Relay, se requiere menos carga de proceso en la red para asegurar que los datos se transportan de manera confiable. Por lo tanto, es lógico el uso de procedimientos simplificados como los de Frame Relay. "Esta tecnología ofrece mejor velocidad y rendimiento porque realiza solamente un

control de errores mínimo; si se produce un error, el protocolo se limita a desechar los datos. Cuando Frame Relay desecha datos erróneos, puede hacerlo sin comprometer la confiabilidad de los datos de usuario porque los niveles superiores de los protocolos transportados sobre esta tecnología proporcionarán la corrección de errores"[21].

El tercer principio básico de Frame Relay es que existe una congestión limitada dentro de la red. Frame Relay supone que existe una cantidad ilimitada de ancho de banda disponible, si se produce una congestion, el protocolo desecha los datos e incluye mecanismos para "notificar explícitamente" al usuario final la presencia de congestión, y confía en que reaccionará ante estas notificaciones explícitas.

f) Mecanismos de Control de la Saturación

Frame Relay se implanta sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos; ya que el control de flujo se puede realizar a través de los protocolos de las capas superiores, la tecnología Frame Relay implanta dos mecanismos de notificación de la saturación:

- FECN (Forward Explicit Congestion Notification).
- BECN (Backward Explicit Congestion Notification).

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de Frame Relay; éste también contiene un bit DE (Discard Eligibility Indicator) que se utiliza para identificar el tráfico menos importante que se puede eliminar durante periodos de saturación.

El bit FECN es parte del campo Address en el encabezado de la trama Frame Relay. "El mecanismo FECN inicia en el momento en que un dispositivo DTE envía una trama Frame Relay a la red; si la red está saturada, los dispositivos DCE fijan el valor del bit FECN de las tramas en 1. Cuando las tramas llegan al dispositivo DTE destino, el campo Address (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino"[22]. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implantación, el control de flujo puede iniciarse o bien la indicación se puede ignorar.

El bit FECN notifica a un DTE que el dispositivo receptor debe iniciar procedimientos para evitar la congestión. Cuando un switch Frame Relay detecta la existencia de congestión en la red, envía un paquete FECN al dispositivo destino, indicando que se ha producido la congestión.

El bit BECN es parte del campo Address en el encabezado de la trama Frame Relay. Los dispositivos DCE fijan el valor del bit BECN en 1 en las tramas que viajan en sentido opuesto a las tramas con bit FECN igual a 1. Esto permite al dispositivo DTE receptor saber que una trayectoria específica en la red está saturada; posteriormente, el dispositivo

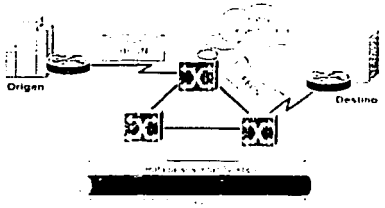
[21] Varios Autores. 1997. Ed. McGraw-Hill. "LAN Times. Guía de Redes de Área Extensa".
[22] Ídem.

DTE envía esta información a un protocolo de las capas superiores para que sea procesada. Dependiendo de la implantación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

El bit BECN notifica a un DTE que el dispositivo receptor debe iniciar procedimientos para evitar la congestión. "Cuando un switch Frame Relay detecta congestión en la red envía un paquete BECN al router origen, instruyéndolo para que reduzca la velocidad a la cual está enviando los paquetes. Si el router recibe un BECN durante el intervalo de tiempo actual, reduce la velocidad de transmisión un 25%"[23].

Los FECN y BECN son activados por la red cuando empieza a detectar que el tráfico aumenta y se debe evitar la congestión (Figura 3.23). Así, todas las tramas que pasan por el nodo, hacia el destino (forward) o hacia el origen (backward), con FECN y BECN activados, se entregan a cada equipo de acceso del usuario.

Figura 3.23: Mecanismos de control de la saturación.



El equipo de acceso que recibe tramas con BECN activo puede reducir la cantidad de información enviada a la red hasta que ya no reciba más. El equipo de acceso conectado en el destino, que recibe tramas con el FECN activo, puede controlar al equipo de acceso conectado en el origen utilizando mecanismos de control de flujo y una ventana de transmisión de niveles superiores. Las tramas con DE activo pueden ser descartadas por la red si sigue existiendo la congestión.

1. Bit DE (Discard Eligibility Indicador)

El bit DE se utiliza para indicar que una trama tiene una importancia menor que otras: este bit es parte del campo Address en el encabezado de la trama Frame Relay.

Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que ésta tiene una importancia menor respecto a las demás tramas. "Al saturarse la red, los dispositivos DCE descartarán las tramas con el bit DE fijado a 1 antes de descartar aquellas que no lo tienen"[24]; lo anterior disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante el período de saturación.

[23] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Segundo Año".
[24] Idem.

Cuando el router detecta congestión de red, el switch Frame Relay descarta en primer lugar los paquetes con el bit DE igual a 1. El bit DE se establece en el tráfico sobresuscrito (es decir, el tráfico recibido después de alcanzar la CIR).

2. Verificación de Errores en Frame Relay

Frame Relay utiliza un mecanismo para la verificación de errores conocido como FCS (Frame Check Sequence). El FCS compara dos valores calculados para determinar si se han presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto directo al implantarse la verificación de errores más que su corrección. Frame Relay por lo general se implanta en medios confiables de transmisión de datos, por lo que la integridad de la información no se sacrifica, ya que la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte más alta de Frame Relay.

g) Implantación de la Red Frame Relay

Una implantación habitual de Frame Relay consiste en equipar un multiplexor T1 con interfaces Frame Relay e interfaces que no sean Frame Relay. El tráfico de Frame Relay es enviado fuera de la interfaz Frame Relay y hacia la red de datos; el tráfico que no es de Frame Relay se direcciona hacia la aplicación o servicio adecuados, como un PBX de servicio telefónico o una aplicación de videoconferencia.

Una red Frame Relay típica consta de varios dispositivos DTE, que pueden ser ruteadores, conectados hacia puertos remotos de un equipo multiplexor vía servicios tradicionales punto a punto, como T1, T1 multipunto o circuitos de 56 Kb (Figura 3.24).

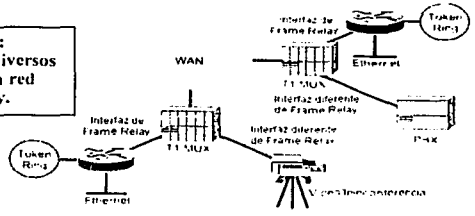


Figura 3.24: Implantación de diversos servicios en una red Frame Relay.

Las líneas que conectan los dispositivos de usuario al equipo de red pueden operar a una velocidad seleccionada de una amplia gama de velocidades de transmisión de datos. Las velocidades entre 56 kbps y 2 Mbps son típicas, aunque Frame Relay puede soportar velocidades inferiores y superiores.

No existe ningún estándar en la actualidad para la conexión cruzada de equipo dentro de una red Frame Relay. Por lo tanto, el soporte de las interfaces Frame Relay no necesariamente implica que se deba utilizar este protocolo entre los servicios de red. De

esta manera, se puede utilizar la conmutación por circuito tradicional, la conmutación por paquetes o un enfoque híbrido que combine estas tecnologías.

La mayoría de las redes Frame Relay que se utilizan en la actualidad son equipadas por los proveedores de servicios que ofrecen servicios de transmisión a clientes; a esto se le conoce como un servicio público de Frame Relay, ya que Frame Relay también se implanta tanto en las redes públicas ofrecidas por las compañías de larga distancia, como en las redes privadas empresariales.

1. Redes Públicas de Larga Distancia

En las redes públicas Frame Relay de larga distancia, el equipo de conmutación utilizado se ubica en las centrales telefónicas de las compañías de larga distancia. En este caso, los usuarios obtienen beneficios económicos implícitos en tarifas sensibles al tráfico y no tienen que invertir tiempo y esfuerzo para administrar y mantener el equipo y el servicio de red.

En general, el proveedor del servicio de telecomunicaciones también es propietario del equipo DCE. El equipo DCE puede ser propiedad del cliente, o bien del proveedor del servicio de telecomunicaciones como un servicio para el usuario.

Actualmente la mayoría de las redes Frame Relay son redes públicas que suministran servicios de larga distancia.

2. Redes Privadas Empresariales

Las organizaciones a nivel mundial están utilizando cada vez más redes privadas Frame Relay; en dichas redes la administración y el mantenimiento son responsabilidad de una empresa (o compañía privada). El cliente es el dueño de todo el equipo, incluyendo el de conmutación.

b) Formato de la Trama Frame Relay

Para entender mejor la funcionalidad de Frame Relay, ayuda mucho conocer la estructura de la trama de esta tecnología.

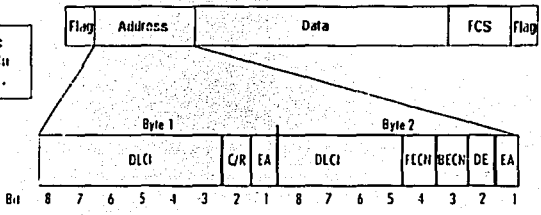
Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes ya que hay una gran variedad de opciones disponibles en la implantación, conocidos como anexos a las definiciones del estándar básico. "La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8,000 bytes, aunque por defecto es de 1,600 bytes"[25].

La trama Frame Relay está formada por tres componentes principales: el área del encabezado y de las direcciones, la porción de los datos de usuario y el FCS. El área de direcciones que tiene una longitud de 2 bytes se compone de 10 bits que representan al

[25] Varios Autores. 1997. Ed. McGraw-Hill. "LAN Times. Guía de Redes de Área Extensa".

identificador del circuito y 6 bits de los campos asociados a la administración de la saturación (Figura 3.25).

Figura 3.25: Formato de la trama FDDI.



- Flags (Delimitadores). Delimitan el comienzo y la terminación de la trama. El valor de este campo siempre es el mismo y se representa como el número decimal 7E o el número binario 01111110.
- Address (Dirección). Indica la longitud del campo de dirección; aunque las direcciones Frame Relay son actualmente todas de 2 bytes de largo, los bits de Dirección ofrecen la posibilidad de extender las longitudes de las direcciones en el futuro. El octavo bit de cada byte del campo Address se utiliza para indicar la dirección. Este campo contiene la siguiente información:
  - DLCI (Data Connection Identifier). Identificador de Conexión del Enlace de Datos. El DLCI de 10 bits es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y DCE. Cada conexión virtual que se multiplexe en el canal físico será representada por un DLCI único. Los valores del DLCI tienen significado local solamente, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual.
  - EA (Address Extension). Dirección Extendida. Se utiliza para indicar si el byte cuyo valor EA es 1 es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte sea el último octeto DLCI. Aunque todas las implantaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCI's más largos. El octavo bit de cada byte del campo Address se utiliza para indicar el EA.
  - C/R (Command/Response field bit). Bit de Orden/Respuesta. El C/R es el bit que sigue después del byte DLCI más significativo en el campo Address. El bit C/R hasta el momento no está definido.
  - Control de la saturación. Este campo consta de 3 bits que controlan los mecanismos de notificación de la saturación en Frame Relay. Estos son los bits FECN, BECN y DE, que son los últimos 3 bits en el campo Address.

- FECN (Forward Explicit Congestion Notification). Notificación de la Saturación Explícita hacia Adelante. Es un campo de un solo bit que puede fijarse en un valor de 1 por medio de un interruptor para indicar a un dispositivo DTE terminal, como un ruteador, que ha habido saturación en la dirección de la transmisión de la trama del origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de reaccionar de manera inteligente ante estos indicadores de saturación.
- BECN (Backward Explicit Congestion Notification). Notificación de Saturación Explícita hacia Atrás. Es un campo de un solo bit que, al establecer su valor a 1 por un switch, indica que ha habido una saturación en la red en la dirección opuesta a la de la transmisión de la trama desde el origen al destino.
- DE (Discard Eligibility Indicator). Bit Elegible para Descartar. Este bit es fijado por el dispositivo DTE, por ejemplo un ruteador, para indicar que la trama marcada es de menor importancia en relación con otras tramas que se estén transmitiendo. En una red saturada las tramas que se marcan como DE, deben ser descartadas antes que cualquier otra. Lo anterior representa un mecanismo justo de establecimiento de prioridad en las redes Frame Relay.

- Data (Datos). Los datos contienen información encapsulada de las capas superiores; cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil que variará en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar el PDU (Protocol Data Unit) a través de una red Frame Relay.
- FCS (Frame Check Sequence). Secuencia de Verificación de Tramas. Asegura la integridad de los datos transmitidos. Este valor es calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión.

3.3.3. X.25

"X.25 surgió por primera vez en 1976 cuando el CCITT de la ITU (International Telecommunications Union) publicó sus recomendaciones para conectar equipos terminales de datos a redes de datos de conmutación de paquetes; esta recomendación se desarrolló principalmente para conectar terminales remotas sin inteligencia a computadoras centrales. Sin embargo, su flexibilidad y confiabilidad hicieron de X.25 una plataforma perfecta para una generación entera de estándares de comunicación de datos.

En 1976, el estándar X.25 admitía una velocidad máxima de transmisión de 64 kbps, desafortunadamente, la sobrecarga debida a la exhaustiva verificación de errores del protocolo consumía la mayoría de este ancho de banda. En 1992, la ITU editó una revisión

del estándar X.25 que, entre otras mejoras, incrementó la velocidad máxima soportada a 2.048 Mbps"[26].

a) Características

X.25 es una interfaz orientada a conexión, es decir establece una conexión previa a la transmisión de datos entre el emisor y el receptor, para una WAN de conmutación de paquetes que utiliza circuitos virtuales para enviar paquetes individuales de datos a su correspondiente destino en la red.

Sin embargo, "por cada conexión realizada sólo se transmite un paquete de datos, lo cual da lugar a uno de los principales problemas de las comunicaciones orientadas a conexión: el colapso de un canal hasta que todos los datos se hayan transmitido"[27]. Por tal motivo, en el caso de X.25 "todos los datos" significa un paquete; al mismo tiempo X.25 mantiene la confiabilidad de las comunicaciones orientadas a conexión.

Si los datos se transmiten a la velocidad de un sólo paquete por conexión, se originan varias miles de conexiones para completar una sola transmisión de datos basada en paquetes. Este elevado número de conexiones y de dispositivos que realizan las transmisiones recibe el nombre de red de conmutación de paquetes. La naturaleza de X.25 de conmutación de paquetes le da la posibilidad de acomodarse a las ráfagas de tráfico que exceden el ancho de banda promedio.

"La sobrecarga en X.25 es exhaustiva, comparada con la mayoría de los protocolos de conmutación de paquetes, lo cual se debe a los rigurosos mecanismos de comprobación de errores y de confiabilidad en la transmisión. En X.25 cada ruteador y conmutador a lo largo del camino de los datos debe recibir completamente cada paquete, comprobar su dirección destino, y a continuación realizar las rutinas de comprobación de errores antes de enviarlo a la siguiente etapa de su viaje"[28]. Como resultado, cada nodo en X.25 mantiene una tabla con información de administración, control de flujo y verificación de errores contra la cual comprueba cada paquete. Además, las estaciones destino en la red X.25 son responsables de la detección de paquetes perdidos o dañados y de solicitar la retransmisión.

X.25 posee una confiabilidad e integridad de datos acorazadas, desempeñando estas labores mediante un proceso intrincado de confirmación de paquetes de datos y comprobación de errores. Cada vez que el transmisor envía un paquete, el receptor debe enviar un paquete de respuesta como contestación; usualmente, aunque el funcionamiento interno de los conmutadores de paquetes X.25 no se encuentra definido por los estándares y por lo tanto es propietario, la mayoría de las redes X.25 requieren de una confirmación a nivel de enlace de datos de cada uno de los nodos a través de los cuales pasa el paquete y de una confirmación a nivel de red por parte del receptor.

[26] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".
[27] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".
[28] Ídem.

b) Capas del protocolo X.25

La especificación para X.25 describe tres capas que corresponden a las tres capas inferiores del modelo OSI y son la capa física, la capa de enlace y la capa de paquete.

1. Capa Física

"La capa física se denomina interfaz X.21, la cual especifica las interfaces eléctrica y física entre una estación y el nodo de conmutación de paquetes en la red X.25"[29]. Aunque X.25 tiene en X.21 su propia interfaz física especializada, en las primeras épocas se utilizaban interfaces RS232-C o V.35 en lugar de X21.

En el estándar se hace referencia a la computadora del usuario como DTE (Data Terminal Equipment) y al nodo de conmutación de paquetes al que está conectado el DTE como DCE (Data Circuit-terminating Equipment).

2. Capa de Enlace

La capa de enlace del modelo X.25 corresponde a la capa de acceso al medio del modelo OSI y se encarga de la transferencia confiable de datos a través del enlace físico mediante la transmisión de los datos como una secuencia de tramas. También describe el tipo de transmisión de datos, así como la composición de la trama de X.25; además de utilizar el protocolo LAP-B (Link Access Procedure-Balanced) para establecer conexiones virtuales, gestionar el control de flujo de una sesión asíncrona balanceada y liberar los circuitos cuando finaliza la transmisión. En este nivel se define la composición de la trama, los procedimientos de control de flujo y los mecanismos de comprobación de errores; LAP-B incluye un método para confirmar la recepción de cada paquete en la estación destino.

3. Capa de Paquete

En la capa de paquete X.25 establece las conexiones virtuales confiables a lo largo de la red de conmutación de paquetes; dichas conexiones virtuales permiten a X.25 proporcionar el envío punto a punto, es decir orientado a conexión, de paquetes de datos en vez del envío no orientado a conexión, o punto multipunto, de paquetes que tiene lugar en otros protocolos de transporte.

Los datos del usuario se mueven hacia abajo al nivel 3 de X.25, que les añade una cabecera consistente en información de control dando lugar a un paquete. La información de control incluida en el paquete tiene varios objetivos, entre los que se encuentran los siguientes:

- Identificación de un circuito virtual dado mediante un número al que se asociarán los datos.
- Definición de números de secuencia para su uso en el control de flujo y de errores entre los circuitos virtuales.

[29] Ramteke.2001. Ed. Prentice-Hall. "Networks".

El paquete X.25 completo se pasa después al protocolo LAP-B que añade información de control al principio y al final del paquete, dando lugar a una trama LAP-B: esta información de control es necesaria para el funcionamiento de dicho protocolo.

En las comunicaciones basadas en paquetes, una unidad de información se fracciona en muchos paquetes de datos más pequeños, cada uno con su propia dirección. El emisor envía estos paquetes a través de la red de comunicaciones hasta el receptor en donde los paquetes son ensamblados, recomponiéndose la unidad de información original para su posterior procesamiento. El equipo que fracciona, gestiona y posteriormente ensambla los paquetes recibe el nombre de PAD (Packet Assembler/Disassembler) y cuenta con múltiples puertos. Además existen tres protocolos adicionales que gobiernan el trabajo interno de un PAD:

- X.3. Especifica realmente como el PAD ensambla y fracciona los paquetes de datos.
- X.28. Define la interfaz entre el DTE y el PAD.
- X.29. Define la interfaz entre el equipo de comunicaciones de datos y el PAD.

c) Circuitos Virtuales en X.25

X.25 permite tanto los SVC como los PVC, lo cual lo hace más flexible que otros protocolos de conmutación de paquetes. Un SVC es un circuito virtual que se establece dinámicamente mediante una petición de llamada y una liberación de la misma. Un PVC es un circuito virtual fijo asignado en la red; la transferencia de los datos se produce como en los SVC's, pero en este caso no se necesita realizar ni el establecimiento ni el cierre de la llamada.

En la figura 3.26 se muestra una secuencia de eventos típica de un SVC. En la parte izquierda de la figura se indican los paquetes intercambiados entre la máquina de usuario A y el nodo de conmutación de paquetes al que está conectada, mientras que la parte derecha muestra los paquetes intercambiados entre la máquina de usuario B y su nodo. El redireccionamiento de los paquetes dentro de la red no es visible al usuario.

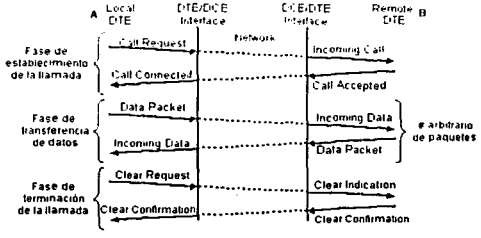


Figura 3.26: Secuencia de eventos del protocolo X.25.

La secuencia de eventos es la siguiente:

1. A solicita un circuito virtual a B mediante el envío de un paquete "Call Request" al DCE de A. El paquete incluye las direcciones de origen y destino así como el número a usar para este nuevo circuito virtual: las demás transmisiones de entrada/salida se identificarán a través de este número de circuito virtual.
2. La red dirige esta petición de llamada al DCE de B.
3. El DCE de B recibe el paquete "Call Request" y envía un paquete "Incoming Call" a B. Este paquete tiene el mismo formato que el "Call Request", pero con un número de circuito virtual diferente: dicho número lo elige el DCE de B del conjunto de números locales libres.
4. B indica la aceptación de la llamada mediante el envío de un paquete "Call Accepted", que especifica el mismo número de circuito virtual que el del paquete "Incoming Call".
5. El DCE de A recibe el paquete "Call Accepted" y envía a A un paquete "Call Connected". Este paquete tiene el mismo formato que el de "Call Accepted", pero el número de circuito virtual es el mismo que el del paquete "Call Request" original.
6. A y B se intercambian paquetes de datos y de control haciendo uso de sus respectivos números de circuito virtual.
7. A (o B) envía un paquete "Clear Request" para liberar el circuito virtual y se recibe un paquete "Clear Confirmation".
8. B (o A) recibe un paquete "Clear Indication" y transmite uno de "Clear Confirmation".

d) Formato del Paquete X.25

En la figura 3.27 se muestran los formatos básicos de paquetes X.25. "Los datos del usuario se segmentan en bloques con un cierto tamaño máximo, añadiéndose a cada segmento un encabezado de 24, 32 o 56 bits para formar un paquete de datos. En el caso de que se utilice un número de secuencia de 15 bits para indicar el circuito virtual, el encabezado comienza con un octeto identificador de protocolo con valor de 00110000"[30].

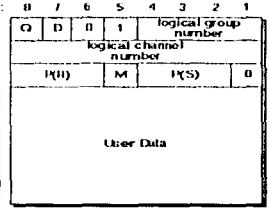
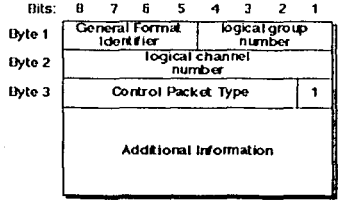


Figura 3.27: Formatos básicos de paquetes en X.25.



a) Paquete de datos estándar. **b) Paquete de control estándar.**

Los campos del paquete de datos (Figura 3.27 (a)) con números de secuencia de 3 bits se describen a continuación:

[30] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

- LCI (Logical Channel Identifier). Identificador de Canal Lógico. Consta de 12 bits utilizados para identificar el número de circuito virtual. Debido a que cada grupo de los 16 posibles puede tener 256 canales, pueden existir un total de 4096 LCI's. Se compone de los siguientes campos:
  - Logical Group Number (Número de Grupo Lógico). Campo de 4 bits que identifica el número de grupo. Permite un total de 2^4 o 16 números de grupo.
  - Logical Channel Number (Número de Canal Lógico). Campo de 8 bits que identifica el número de canal. Permite 2^8 o 256 números de canales.
- Bit Q (Qualifier). Bit Calificador. Determina si un paquete es enviado hacia el DTE remoto o simplemente al PAD remoto. Lo utiliza el usuario para distinguir entre dos tipos de datos.
- Bit D (Delivery). Bit de Entregado. Especifica si el acuse de recibo es local o extremo a extremo.
- P(S) (Sending Packet Number). Número de Paquete Enviado. Se utiliza para el control de flujo de errores a través del circuito virtual y contiene el número del paquete enviado.
- P(R) (Receiving Packet Number). Número de Paquete Recibido. Se usa, al igual que el campo P(S), para el control de flujo de errores a través del circuito virtual y contiene el número del siguiente paquete que el emisor debe enviar.
- Campo M (More Packets). Campo de Más Paquetes. Simplemente indica al extremo remoto si se esperan recibir más paquetes o no. Este campo es usado por las capas superiores para segmentar (o descomponer las unidades de información en unidades más pequeñas) y ensamblar las unidades de información.
- User Data (Datos de Usuario). Contiene los datos del usuario que serán transmitidos.

Además de la transmisión de datos del usuario, X.25 debe transmitir información de control relativa al establecimiento, mantenimiento y liberación de circuitos virtuales; esta información se transmite en paquetes de control (Figura 3.27 (b)), cada uno de los cuales incluye los siguientes campos:

- GFI (General Format Identifier). Identificador de Formato General. Se compone de los bits Q y D que tienen el mismo significado que en el paquete de datos, así como de 2 bits extras, los cuales determinan si el modo de transmisión es de control normal o extendido. Identifica los parámetros del paquete; por ejemplo si el paquete transporta datos del usuario o información de control, qué tipo de ventaneo se está utilizando y qué tipo de confirmación de entrega se requiere.
- LCI (Logical Channel Identifier), Identificador de Canal Lógico. Se compone de los campos Logical Group Number y Logical Channel Number y tiene el mismo significado que en el paquete de datos.
- Control Packet Type (Tipo de Paquete de Control). Campo de 7 bits que identifica la función de control específica.

- Additional Information (Información de Control Adicional). Contiene información complementaria relacionada con le función de control especificada en el campo Control Packet Type.

En la tabla 3.2 se describe brevemente la función de los diferentes tipos de paquetes en X.25.

Tabla 3.2: Tipos de paquetes en X.25

Tipo de paquete	Dirección	Servicio		Descripción
		VC	PVC	
Establecimiento y liberación de la llamada				
CALL REQUEST INCOMING CALL	DTE→DCE DCE→DTE	X X		Solicitud de conexión DTE-DTE y el tipo de recursos necesarios para la llamada.
CALL ACCEPTED CALL CONNECTED	DTE→DCE DCE→DTE	X X		Confirmación del establecimiento de la conexión DTE-DTE con los recursos permitidos.
CLEAR REQUEST	DTE→DCE	X		Solicitud de liberación de los recursos de la red asignados a una llamada en especifico.
CLEAR INDICATION	DCE→DTE	X		Informa al DTE de la solicitud de liberación.
DTE CLEAR CONFIRMATION	DTE→DCE	X		Informa a la red que el DTE ha terminado la llamada en especificada.
DCE CLEAR CONFIRMATION	DCE→DTE	X		Informa al DTE que la red ha terminado la llamada especificada.
Rearranque				
DTE RESTART REQUEST	DTE→DCE	X	X	Solicitud de terminación de todas las llamadas de una interfaz.
DTE RESTART INDICATION	DCE→DTE	X	X	Informa al DTE que la red terminará todas las llamadas de la interfaz especificada.
Diagnóstico				
DIAGNOSTIC	DCE→DTE	X	X	La red provee información de diagnóstico para el seguimiento y la recuperación de errores.
REGISTRATION REQUEST	DTE→DCE	X	X	El usuario solicita a la red la suscripción a los recursos de una red en especifico.
REGISTRATION CONFIRMATION	DCE→DTE	X	X	Información de las acciones realizadas por la red respecto a la solicitud hecha por el usuario.
Datos e interrupciones				
DTE INTERRUPT DCE INTERRUPT	DTE→DCE DCE→DTE	X X	X X	Interrupción explicita de la secuencia en el envío de información de equipo terminal a equipo terminal (end-to-end) desde el DTE o el DCE.
DTE INTERRUPT CONFIRMATION	DTE→DCE	X	X	Respuesta equipo terminal a equipo terminal (end-to-end) desde el DTE al paquete INTERRUPT.
DCE INTERRUPT CONFIRMATION	DCE→DTE	X	X	Respuesta equipo terminal a equipo terminal (end-to-end) desde el DCE enviando el paquete DTE INTERRUPT.
DTE DATA	DTE→DCE	X	X	Datos del usuario o de los protocolos de las capas superiores enviados desde el DTE.
DCE DATA	DCE→DTE	X	X	Datos del usuario o de los protocolos de las capas superiores enviados desde el DTE remoto por la ruta del DCE local.
Control de flujo y reinicio				
DTE RR (Receive Ready)	DTE→DCE	X	X	Reconocimiento de los paquetes de datos y permisos para enviar más desde el DTE.
DCE RR (Receive				Reconocimiento de los paquetes de datos y

Ready)	DCE→DTE	X	X	permisos para enviar más desde el DCE.
DTE RNR (Receive Not Ready)	DTE→DCE	X	X	DTE solicita al DCE detener el flujo de paquetes de datos.
DCE RNR (Receive Not Ready)	DCE→DTE	X	X	DCE solicita al DTE detener el flujo de paquetes de datos.
DTE REJECT	DTE→DCE	X	X	Solicitud al DCE para la retransmisión de paquetes de datos comenzando desde un número de secuencia específico.
RESET REQUEST RESET INDICATION	DTE→DCE DCE→DTE	X X	X X	Solicitud de reinicialización de los números de secuencia de los paquetes de datos sobre un PVC o SVC específico e informa al DTE que la red ha reinicializado estos números.
DTE/DCE RESET CONFIRMATION	DTE→DCE	X	X	Informa al DTE o al DCE que los números de secuencia han sido reinicializados.

Un DTE puede enviar un paquete "Interrupt" que detenga el control de flujo de los paquetes de datos, dicho paquete se envía a través de la red hacia el DTE destino con una prioridad superior que los paquetes de datos en tránsito.

e) Multiplexaje

Quizá el servicio más importante ofrecido por X.25 sea el multiplexaje, un DTE puede establecer hasta 4.095 circuitos virtuales simultáneamente con otros DTE sobre el mismo enlace físico DTE-DCE. El DTE puede asignar internamente estos circuitos como le plazca. La línea DTE-DCE permite el multiplexaje Full-Duplex, es decir, un paquete asociado a un circuito virtual dado se puede transmitir en ambos sentidos en cualquier instante de tiempo.

Mediante el multiplexaje X.25 permite que múltiples usuarios se comuniquen con otros muchos usuarios de manera simultánea a través de la misma red de conmutación de paquetes, lo cual significa que cualquier sistema con un punto de acceso a la nube X.25 puede enviar paquetes a cualquier otro sistema que tenga acceso a dicha nube.

Para saber qué paquetes pertenecen a cada circuito virtual, cada paquete contiene un número de circuito virtual de 12 bits. El número 0 se reserva siempre para paquetes de diagnóstico comunes a todos los circuitos virtuales, se usan rangos contiguos de números para cuatro categorías de circuitos virtuales. A los circuitos virtuales permanentes se les asignan números que comienzan con 1. La siguiente categoría la constituyen las llamadas virtuales entrantes, lo que significa que sólo a las llamadas procedentes de la red se les puede asignar estos números"[31]. Por el contrario, el circuito virtual se da en los dos sentidos. Cuando se recibe una solicitud de llamada, el DCE selecciona un número libre de esta categoría.

Las llamadas salientes en un solo sentido se inician por parte del DTE, de tal manera que él elige uno de los números libres reservados para estas llamadas; esta separación de categorías está pensada para evitar la selección simultánea por parte del DTE y del DCE del mismo número para dos circuitos virtuales diferentes.

[31] Ídem.

La categoría de llamadas virtuales en ambos sentidos prevé un desbordamiento para la reserva compartida por el DTE y el DCE, lo que permite diferencias en los picos de flujo de tráfico.

f) Control de Flujo y de Errores

El control de flujo y de errores en el nivel de paquete de X.25 es básicamente idéntico en formato y funcionamiento al control de flujo realizado por el protocolo HDLC. "Se hace uso de un protocolo de ventana deslizante en el que cada paquete incluye un número de secuencia correspondiente al paquete enviado P(S), y un número de secuencia relativo al paquete recibido P(R). Aunque por default se utilizan números de secuencia de 3 bits, un DTE puede solicitar, de forma opcional, a través del mecanismo de facilidades de usuario el empleo de números de secuencia de 7 o de 15 bits.

El campo P(S) se asigna por parte del DTE a los paquetes salientes de acuerdo con el circuito virtual al que se asocian, es decir, el campo P(S) de cada nuevo paquete de salida sobre un circuito virtual es uno más que el del paquete anterior de ese circuito, modulo 8 (o modulo 128 o modulo 32.768). El campo P(R) contiene el número del siguiente paquete esperado por el otro extremo de un circuito virtual dado, siendo usado para la confirmación en la técnica de incorporación de confirmaciones. Si uno de los extremos no dispone de datos que enviar, puede llevar a cabo la confirmación de los paquetes recibidos mediante los paquetes de control RR (Receive Ready) y RNR (Receive Not Ready), cuyo significado es el mismo que en el protocolo HDLC. El tamaño implícito de ventana es 2, pudiendo llegar a ser igual a 7 o a 32.767 para números de secuencia de 7 bits y de 15 bits respectivamente"[32].

El mecanismo de confirmación (en forma del campo P(R) en los datos o a través de los paquetes RR y RNR) y en consecuencia el control de flujo, puede tener significado local o extremo a extremo de acuerdo con el valor del bit D. Si D=0 (situación usual), la confirmación tiene lugar entre el DTE y la red, lo cual se usa por el DCE local y/o la red para confirmar la recepción de paquetes y realizar el control de flujo desde el DTE hacia la red; si D=1 las confirmaciones proceden del DTE remoto.

El esquema de control de errores consiste en la técnica ARQ go-back-N, las confirmaciones negativas se llevan a cabo en forma de paquetes de control (REJ, Reject), de modo que si un nodo recibe un paquete de este tipo retransmitirá el paquete especificado y todos los siguientes.

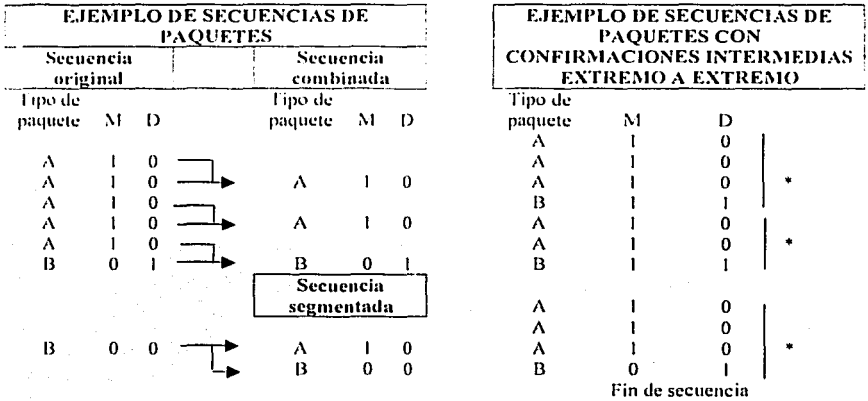
[32] Idem.

g) Secuencia de Paquetes

X.25 posibilita la identificación de secuencias contiguas de paquetes de datos, lo que se conoce como "***secuencia completa de paquetes***", dicha característica presenta varios usos, el principal es su empleo en la interconexión de redes para permitir el envío de bloques de datos de tamaño mayor al permitido por la red sin que pierdan su integridad.

Para especificar este mecanismo, "X.25 define dos tipos de paquetes: paquetes A y paquetes B. Un **paquete de tipo A** es aquel en el que el bit M toma el valor de 1, el bit D el valor 0 y el paquete está completo (su longitud es la máxima permitida). Un **paquete tipo B** es cualquier paquete que no sea tipo A; así una secuencia completa de paquetes consiste en cero o más paquetes A seguidos de un paquete tipo B"[33]. La red puede combinar esta secuencia para construir paquetes más grandes, asimismo la red puede dividir un paquete de tipo B en paquetes de menor tamaño para producir una secuencia completa de paquetes.

Figura 3.28: Secuencias de paquetes X.25.



La forma en que se gestiona el paquete B depende del valor de los bits M y D. Si D=1, el DTE receptor envía una confirmación extremo a extremo hacía el DTE emisor, lo que indicaría una confirmación de la secuencia completa de paquetes. Si M=1, existen secuencias de paquetes completas adicionales; esto posibilita la creación de subsecuencias como parte de una secuencia más larga, de modo que se puede producir la confirmación extremo a extremo antes de que finalice la secuencia más larga.

[33] Ídem.

La figura 3.28 muestra algunos ejemplos acerca de estos conceptos. Es responsabilidad de los DCE reorganizar los cambios en la numeración de la secuencia causados por la segmentación y llevar a cabo la agrupación o ensamblado.

h) Reinicio y Rearranque

X.25 proporciona dos facilidades para la recuperación de errores. "la facilidad de reinicio se usa para reiniciar un circuito virtual, lo que significa que los números de secuencia se igualen a 0 en ambos extremos y que se pierdan los paquetes de datos o de interrupción en tránsito"[34]. Es función de un protocolo de nivel superior la recuperación de los paquetes perdidos: un reinicio puede provocarse por diversas condiciones de error tales como la pérdida de paquetes, errores en el número de secuencia, congestión o pérdida de un circuito virtual interno en la red. En este último caso ambos DCE deben restablecer el circuito virtual interno para atender al circuito virtual externo aún existente entre los dos DTE. Tanto un DTE como un DCE pueden originar un reinicio a través del uso de un paquete (Reset Request) o un (Reset Indication), a los cuales responderá el receptor con un paquete (Reset Confirmation). Independientemente de quien origine el reinicio, es responsabilidad del DCE involucrado informar al otro extremo.

"Una situación de error más seria requiere un rearranque: el envío de un paquete (Restart Request) es equivalente a la emisión de un paquete (Clear Request) sobre todas las llamadas virtuales y uno de (Reset Request) sobre todos los circuitos virtuales, tanto el DCE como el DTE pueden iniciar la acción"[35]. Un ejemplo de una condición de rearranque consiste en la pérdida temporal del acceso a la red.

[34] Ramteke,2001. Ed. Prentice-Hall. "Networks".
[35] Idem.

CAPÍTULO 4

Fundamentos de Seguridad en los Sistemas de Cómputo

4.1. Importancia de la Seguridad

Para la administración de empresas la información constituye un recurso organizacional muy importante; no obstante, para que dicha información pueda ser útil y oportuna, debe estar disponible en cualquier momento y en cualquier lugar.

Un fraude en las comunicaciones de datos representa la alteración, modificación o intercepción de mensajes con fines de lucro, mediante el uso de un sistema de comunicaciones en línea. Sin importar el medio utilizado, las líneas de telecomunicaciones siempre son vulnerables y están expuestas a un sinfín de peligros como la intercepción y accesos ilícitos.

En los primeros años, los ataques involucraban poca sofisticación técnica, los ataques internos se basaban en utilizar permisos para alterar la información; los externos se basaban en accesar a la red simplemente averiguando una clave válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar vulnerabilidades en el diseño, configuración y operación de los sistemas, lo cual permitió a los nuevos atacantes tomar el control de sistemas completos, produciendo desastres muy serios que en muchas ocasiones llevaron a la desaparición de aquellas organizaciones o empresas con un alto grado de dependencia tecnológica.

Como capital de la empresa cada vez es más importante mantener la seguridad de la información, pero también los riesgos son cada vez mayores. "La protección de la información es más grave desde la aparición de las redes telemáticas. Estas redes y especialmente Internet, hacen que la información sea un problema global y no aislado a las máquinas internas de la empresa"[1]. Las tecnologías aplicadas a la seguridad en redes están en su fase de desarrollo inicial, especialmente por dos motivos:

- La mayoría de sistemas operativos están pensados para arquitecturas mainframe/terminal y no para arquitecturas cliente/servidor o Internet/Intranet que se utilizan actualmente.
- No existen estándares ni organizaciones mundiales aceptadas por todas las empresas proveedoras de seguridad.

[1] Gratton, Pierre. 1998. Ed. Trillas. "Protección Informática".

La seguridad en las redes está relacionada con la seguridad de los sistemas, programas y datos cuando estos existen en una red establecida. El mismo factor que hace que las redes sean útiles, también contribuye a incrementar la probabilidad de que se produzcan brechas en la seguridad. Los efectos de "compartir información" en las redes tienen como resultado la existencia de más usuarios potenciales que accesan al sistema o interceptan datos en la red accesando de forma ilegal a los datos y a los recursos desde una localización remota. El hecho de que la información tiene que viajar de un lugar a otro también incrementa la posibilidad de errores y corrupción.

Los principios clave de la integridad de los datos son: "los datos que están almacenados deben ser exactamente los mismos que los introducidos inicialmente o modificados por última vez; las computadoras, los periféricos y los componentes necesarios para crear la información deberán funcionar correctamente y los datos deberán estar a salvo de otras personas que los pudieran utilizar en beneficio propio"[2].

La integridad y seguridad de los datos están estrechamente relacionadas por su propósito de proteger los datos de peligros potenciales; en el caso de la integridad, el peligro es, a menudo, un simple error de cálculo, confusiones o errores cometidos por personas o fallos de equipos que provocan la pérdida de los datos, corrupción o su incorrecta modificación. En relación con la seguridad, la gente puede tratar de infiltrarse de forma intencionada en los sistemas de otras compañías para robar o estropear información para su beneficio propio.

4.2. Conceptos Básicos Sobre Seguridad

4.2.1. Definición de Integridad y Seguridad

La integridad de los datos es un término utilizado para describir su estado en relación con su pérdida o corrupción; de forma general significa que se puede confiar en que los datos están seguros y son correctos. Una integridad de datos comprometida o pobre implica que dichos datos pueden ser incorrectos o incompletos.

El diccionario define integridad como un estado inalterado y la cualidad o el estado de estar completo o ser indivisible. El objetivo de la integridad de los datos es mantener los datos y la información de los sistemas de computadoras en un estado completo e inalterado; lo cual significa que los datos no podrán ser modificados o perdidos por hechos accidentales o intencionados. Una pérdida de la integridad de los datos significa que ha pasado algo cuyo resultado ha sido su pérdida o modificación.

El término seguridad de los datos describe su estado en relación con su pérdida o destrucción intencional.

[2] Varios Autores. 1998. Ed. McGraw-Hill. "Guía LAN TIMES de Seguridad e Integridad de Datos".

El diccionario define seguridad como la cualidad o el estado de estar libre de daño y como las medidas de protección tomadas contra el espionaje, el sabotaje, el crimen, el ataque o la fuga.

4.2.2. Definición de Confidencialidad

Confidencialidad es el concepto consistente en evitar que la información sensible sea accesible a personas no autorizadas. El problema existente cuando se envía información a través de una red, es que los datos se encuentran expuestos públicamente a otras computadoras conectadas a la red que retransmiten el mensaje al destino final. Es necesario transformar la información de alguna manera que únicamente le proporcione significado al verdadero receptor, es decir, hay que cifrar los datos.

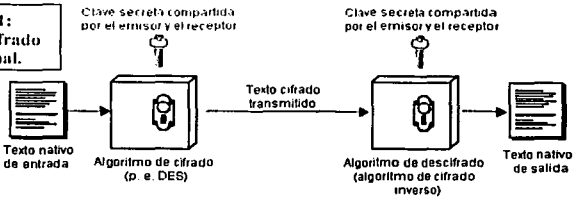
4.2.3. Concepto de Cifrar

Cifrar hace referencia al proceso de desordenar los datos de manera que adquieran una apariencia aleatoria, sin sentido y al mismo tiempo que conserven una forma recuperable. El receptor del mensaje cifrado puede deshacer la alteración o descifrar el mensaje trastocado recuperando su forma original y comprensible. Este concepto constituye la base de la ciencia de la criptografía (literalmente procedente de los términos griegos "escritura secreta").

4.2.4. Definición de Clave, Texto Plano y Texto Cifrado

El método de transformar los datos (algoritmo de cifrado) es, por norma general, completamente público. Solamente se utilizan unos cuantos algoritmos de cifrado, como DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) y RSA (Rivest, Shamir and Adlman). Estos algoritmos reciben la información original que se desea proteger, denominada *texto plano, texto original o texto nativo* y la transforman utilizando un operador matemático denominado *clave*. La versión transformada resultante recibe el nombre de *texto cifrado*. Aunque otros conocieran el algoritmo exacto de cifrado empleado, si quisieran descifrar el texto cifrado deberían disponer de la clave correcta para recrear el texto original (Figura 4.1).

Figura 4.1: Modelo de cifrado convencional.



4.2.5. Concepto de Amenazas, Vulnerabilidades y Ataques

Una amenaza a un sistema de cómputo se define como "una ocurrencia potencial maliciosa o de otra índole, que puede tener un efecto indeseable en los programas y/o recursos asociados con una computadora"[3]; una amenaza es algo malo que puede ocurrir. El concepto de amenaza es significativo debido a que la meta generalmente aceptada de la seguridad en un sistema de cómputo es proveer procesos, técnicas y metodologías que pueden ser utilizadas para reducir las amenazas, lo cual se logra generalmente a través de recomendaciones que guían a los diseñadores de sistemas de cómputo, desarrolladores, usuarios y administradores a evitar ciertas características no deseables del sistema llamadas vulnerabilidades.

Una vulnerabilidad es una característica desafortunada que permite que ocurra una amenaza potencial; en otras palabras, la presencia de vulnerabilidades permite que ocurran cosas malas en un sistema de cómputo.

Un ataque a un sistema de cómputo "es cualquier acción realizada por un intruso malicioso que involucra la explotación de ciertas vulnerabilidades provocando que se lleve a cabo una amenaza existente"[4].

4.3. Amenazas en las Comunicaciones de Datos

La posibilidad de que un intruso logre infiltrarse en una red depende de muchos factores, entre los cuales podemos mencionar los conocimientos técnicos que pudiera tener sobre telecomunicaciones y computación, así como la disponibilidad de equipo sofisticado que permita interceptar y penetrar en una red de comunicaciones.

Considerado que la amenaza básica a un sistema de cómputo dado consiste en que un intruso robe información valiosa almacenada en alguna parte; se debe analizar el sistema con el fin de que todas las posibles vulnerabilidades asociadas con dicho robo puedan ser identificadas y resueltas. Por ejemplo, un password débil o la ausencia de éste en alguna cuenta de usuario es una vulnerabilidad que debería ser examinada.

4.3.1. Acciones Ilegales en los Sistemas de Cómputo

Las acciones ilegales más comunes en los sistemas de cómputo son:

1. La usurpación de puestos. Los impostores tratan de obtener por cualquier tipo de medio el código de identificación del usuario, a fin de conseguir la información necesaria. Si el criminal obtiene la contraseña, suplantará al usuario autorizado para tener acceso a la información de la computadora.
2. La intercepción de líneas telefónicas. El impostor trata de interceptar la línea telefónica para escuchar la información transmitida sin modificarla.

[3] Idem.
[4] Idem.

3. La suplantación de personalidad. El impostor introduce una terminal ficticia entre la computadora y el usuario para interceptar los datos de entrada enviados por el usuario, modificarlos o reemplazarlos y luego retransmitirlos a la computadora. En algunos casos, el impostor transmite un mensaje de error para hacer creer al usuario que el sistema no está disponible.
4. La intercepción de las comunicaciones. El impostor introduce una terminal ilegal en la red para infiltrarse en el sistema cuando algún usuario autorizado establece una comunicación legal. El impostor aprovecha los momentos de inactividad del usuario autorizado para entrar a la red y realizar sus fechorías.
5. La usurpación de líneas de transmisión. El impostor introduce una terminal en la línea para interceptar la transmisión de los datos cuando el usuario autorizado indica a la terminal las instrucciones de la salida de la comunicación. En este momento, el impostor intercepta las instrucciones y envía un mensaje de error para hacer creer al usuario que la línea no está disponible.

4.3.2. Fuentes de las Amenazas a la Integridad

Las fuentes más comunes de amenazas a la integridad de los datos se muestran en la figura 4.2 y son:

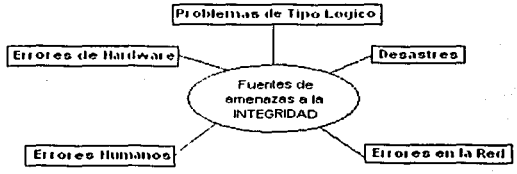


Figura 4.2: Fuentes de amenazas a la integridad.

a) Humanos. El mayor punto débil de los sistemas distribuidos es la gente que los utiliza; la confiabilidad de la raza humana es un manantial de errores inexplicables que parece nunca secarse. Entre las amenazas más comunes de las personas a la integridad de los datos están:

- Accidentes. Errores al momento de introducir datos, así como oprimir una tecla errónea que provoque la pérdida de información.
- Inexperiencia. Falta de personal suficientemente capacitado para operar el sistema.
- Estrés, pánico. El personal no está capacitado para trabajar bajo presión.
- Falta de comunicación. No existe una adecuada coordinación de las actividades realizadas por los integrantes del sistema.
- Venganza. A veces, los empleados que han sido despedidos de la compañía intentarán dañarla destruyendo los datos más importantes mientras permanece en su puesto de trabajo.
- Avaricia. Las ganancias financieras influyen de manera negativa en muchas personas, lo que provoca un mal uso de la información.

b) ***Errores de Hardware.*** Cualquier clase de maquinaria de alto rendimiento sólo puede funcionar adecuadamente durante un cierto tiempo, lo cual incluye a los componentes de las computadoras, así como a los equipos de comunicaciones. Algunas de las fallas eléctricas y mecánicas más comunes de las computadoras son:

- Fallos de disco. Una de las fallas de procesamiento más comunes es el desperfecto de un disco duro.
- Fallas en los controladores de E/S. Cuando un controlador falla, los datos escritos en el disco ya están en mal estado y no existe ningún proceso conocido que permita su recuperación. Las fallas en los controladores no son muy comunes, pero ocurren esporádicamente.
- Fallas de energía. Puede ser de dos tipos: cuando se pierde la energía de la fuente de alimentación que suministra corriente a la máquina o falla la fuente de alimentación de la propia máquina; en cualquier caso, la posibilidad de perder o corromper datos es significativa debido al comportamiento impredecible del sistema cuando falla la energía; asimismo, los datos de la memoria no permanente se pierden cuando de repente desaparece la energía del sistema. Es recomendable instalar fuentes de alimentación ininterrumpida y sistemas con baterías de reserva en los servidores, con el fin de apagar adecuadamente el sistema antes de que se pierda completamente la energía.
- Fallas de memoria. Los circuitos integrados de memoria fallan ocasionalmente, lo cual puede alterar los datos por causas que son imposibles de ver y determinar. Los servidores que incorporan rutinas para verificar la paridad de la memoria son muy útiles para combatir este tipo de problemas, ya que identifican los segmentos de código incorrectos en la memoria e impiden su ejecución.
- Fallas en medios o dispositivos. Los datos almacenados en medios extraíbles para realizar y recuperar copias de seguridad contienen copias de los datos; cualquier problema con estos dispositivos de almacenamiento podría tener como consecuencia la pérdida de datos si el servidor también estuviera caído o dañado. Los problemas con los dispositivos de cinta donde se almacenan copias de seguridad son extremadamente comunes.
- Mal funcionamiento de los chips y de la tarjeta madre. Debido al desgaste sufrido por el paso del tiempo, estos componentes llegan a presentar anomalías en su funcionamiento.

c) ***Errores en la Red.*** En una red los datos se transfieren de una máquina a otra a grandes velocidades; las señales eléctricas son generadas en una computadora y difundidas en algún tipo de red. Las líneas que conectan las máquinas están expuestas a una variedad de riesgos, incluyendo interferencias y averías físicas. Algunas de las formas incorrectas de funcionamiento más comunes que causan la pérdida de datos son:

- Fallas en los controladores y en las tarjetas de red. En el caso de que la tarjeta de red falla en un servidor, es probable que las sesiones remotas se congelen y seguramente los datos no guardados se perderán.

- Problemas en componentes de la red. Los dispositivos de comunicaciones de datos como los routers y los switches pueden tener problemas de memoria o de alto procesamiento, lo cual repercutirá en una excesiva lentitud en la transferencia de información.
- Problemas de radiación. Puesto que todo lo que sucede en una computadora se fundamenta en el movimiento de los electrones, y puesto que la radiación tiene la capacidad de mover electrones, se deduce que la radiación y las computadoras pueden combinarse y provocar que los datos sean incorrectos.

*d) **Problemas de Tipo Lógico**.* El software también puede contribuir a la pérdida de la integridad de los datos; algunas formas comunes son:

- Errores. Los errores abarcan un amplio rango de defectos relacionados principalmente con la lógica de la aplicación. Como cliente se puede hacer poco para protegerse de los errores, porque ninguna empresa de desarrollo de software puede probar todas las posibles opciones de utilización del producto.
- Corrupción de archivos. Los archivos pueden corromperse debido a problemas físicos o de la red, por problemas del control del sistema o de la lógica de la aplicación. Si el archivo corrompido es utilizado por otros procesos para crear datos, el resultado puede ser incorrecto. Este problema es difícil de resolver ya que el usuario final desconoce cuáles son los archivos que intervienen en todo el proceso.
- Errores de intercambio. El intercambio de archivos entre aplicaciones sucede a menudo. Cada vez que los datos intervienen en un proceso de conversión, tal como sucede entre dos procesadores de texto diferentes, la integridad de los datos está en riesgo.
- Errores de almacenamiento. Cuando el disco duro de una máquina se llena puede provocar que los nuevos datos no sean almacenados por falta de recursos, en consecuencia la información quedará incompleta. Incluso la máquina puede apagarse repentinamente ya que intentará escribir en el disco y no lo podrá hacer.
- Errores del sistema operativo. Todos los sistemas operativos tienen su propio conjunto de errores; considerando la complejidad de los sistemas operativos no debería ser sorprendente encontrar alguno de ellos.
- Requisitos mal definidos. Si los requisitos de software no describen correctamente el trabajo que el usuario necesita realizar, el sistema podría generar datos incorrectos. Si el código de comprobación de errores del sistema no detecta alguna anomalía se creará información incorrecta.

*e) **Desastres**.* El medio ambiente puede provocar contingencias que impidan el acceso a la información de manera oportuna. Entre los desastres más comunes se encuentran:

- Incendios.
- Inundaciones.
- Tormentas.
- Accidentes industriales.

- Sabotaje / Terrorismo.

4.3.3. Clasificación de las Amenazas

Las amenazas se clasifican en tres diferentes categorías: divulgación de información, integridad de datos y negación de servicios al sistema de cómputo (figura 4.3).

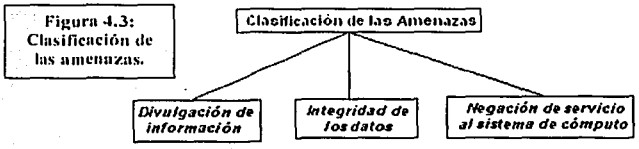


Figura 4.3: Clasificación de las amenazas.

Esta clasificación provee un marco sencillo para la organización de las ideas respecto a la seguridad: es decir, si todas las cosas malas que pueden ocurrir pertenecen a alguno de los tres tipos de amenazas mencionados anteriormente, entonces se provee un primer paso en la comprensión del problema de seguridad y consecuentemente su solución.

a) Divulgación de Información

La amenaza de divulgación de información involucra la difusión de datos a un individuo que no debería tener conocimiento de ellos. En el contexto de la seguridad en cómputo, esta amenaza ocurre cuando algún secreto que está almacenado en una computadora o está en tránsito en la red es descubierto por alguien que no debería conocer dicho secreto.

En las pasadas 2 décadas se ha puesto mucha atención en la amenaza de divulgación entre la comunidad de seguridad en cómputo; de hecho, la mayoría de las investigaciones y desarrollos en seguridad en cómputo se han enfocado específicamente sobre esta amenaza. Una de las principales razones para ponerle mayor énfasis ha sido la importancia que los gobernantes ha puesto para detener esta amenaza.

b) Integridad de los Datos

La amenaza contra la integridad involucra cualquier cambio no autorizado a la información almacenada en un sistema de cómputo; cuando un intruso maliciosamente altera la información, se dice que la integridad de dicha información ha sido comprometida, también se dice que la integridad ha sido comprometida si un error inocente se refleja en un cambio no autorizado. Los cambios autorizados son aquellos que son hechos por ciertas personas con fines justificables.

c) Negación de Servicio al Sistema de Cómputo

La amenaza de negación de servicio ocurre cuando el acceso a los recursos de un sistema de cómputo es bloqueado intencionalmente como resultado de una acción maliciosa

realizada por otro usuario; esto es, si un usuario necesita accesar a un servicio y otro usuario realiza alguna acción maliciosa para prevenir tal acceso, se dice que una negación de servicio ha ocurrido. El bloqueo actual puede ser permanente, con lo que el recurso deseado nunca será provisto o puede provocar que el recurso deseado se retrase demasiado haciéndolo un recurso inútil. En tales casos, se dice que el recurso se ha vuelto inservible.

4.3.4. Tipos de Amenazas Contra la Seguridad

Los diferentes tipos de sistemas en uso hacen virtualmente imposible implantar medidas de seguridad consistentes a través de todos ellos dentro de la organización, y una seguridad centralizada de la red es intrínsecamente comprometida. Los tipos básicos de amenazas contra la seguridad se muestran en la figura 4.4 y son:

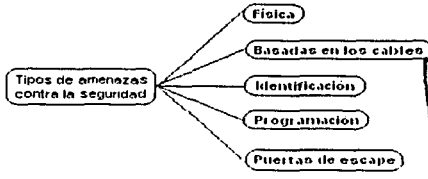


Figura 4.4: Amenazas contra la seguridad.

a) Física. La seguridad física es un concepto bastante sencillo: no se debe dejar a nadie conseguir lo que tiene, ni tampoco permitir el espionaje. Las amenazas de seguridad física más comunes son:

- Robo. Hurto del equipo físico.
- Espionaje. Captura de contraseñas con el fin de comprometer a la organización.
- ID falsos. Falsificación de códigos de seguridad.

b) Basadas en los Cables. La utilización de redes de computadoras crea amenazas adicionales de seguridad para los datos. Los problemas más comunes son:

- Escuchas. La naturaleza del proceso distribuido se basa en la comunicación de diversas computadoras a través de un medio físico; se deduce que se podría escuchar el tráfico de una sesión y capturar dicha información, este tipo de escuchas no necesitan que el dispositivo utilizado esté conectado físicamente a la red, a veces es posible recoger las señales de las radiaciones emitidas a través del cable. Dada la naturaleza confidencial de las comunicaciones que tienen lugar dentro de una empresa, se desearía utilizar alguna técnica de cifrado para evitar que los mensajes sean fácilmente decodificados.
- Marcación a un número telefónico. Cualquier persona con un módem y un número telefónico al cuál llamar puede intentar accesar a una red.
- Imitación. Se refiere a la capacidad de una máquina de parecerse a otra dentro de una red. Esto no es fácil de realizar y significa que seguramente alguien dentro de la organización que conoce la red y los procedimientos de operación está involucrado.

c) ***Identificación***. Hace referencia al proceso por el que una computadora determina si alguien está autorizado a solicitar o dar ciertos servicios al servidor.

- Captura de contraseñas. La captura de contraseñas es una de las argucias que pueden considerarse realmente inteligentes en temas de procesamiento relacionadas con la idea de imitación.
- Averiguación de contraseñas. A través del espionaje o por medio de un software que permita detectar y/o descifrar contraseñas.
- Suposiciones hechas con algoritmos. El filtrado de contraseñas funciona bajo una serie de requisitos que alguien ha codificado en alguna parte y están basados en algún tipo de algoritmo. Puede ser posible que estos algoritmos no funcionen correctamente para un determinado conjunto de datos.
- Edición de contraseñas. La edición de contraseñas requiere una brecha de seguridad interna; de forma sencilla, alguien dentro de la compañía establece una cuenta ficticia o cambia la contraseña de una cuenta inactiva. De esta forma, la máquina puede ser accesada por cualquiera que conozca el usuario y la contraseña de dicha cuenta.

d) ***Programación***. Las violaciones contra la seguridad más peligrosas proceden del código; generalmente los virus amenazan tanto la seguridad como la integridad de los datos. Las diversas variantes de código malicioso son:

- Virus. Un virus es un trozo de programa que se reproduce a sí mismo, accesando a otros programas en la máquina y transfiriéndose a otras máquinas cuando el programa se traslada a ellas; dicho traslado puede ser realizado desde Internet, a través de disquetes o por cualquier otro medio que se introduzca en la máquina.
- Códigos bomba. La idea de los códigos bomba es que a una determinada fecha y hora, o basados en una secuencia de operaciones de la máquina, el código bomba se ejecutará automáticamente afectando el desempeño de la misma.
- Caballos de troya. Es un término general que se aplica a un rango de amenazas de códigos malévolos que incluyen virus, bombas, gusanos, etc. Un caballo de troya se instala por sí mismo en una máquina y hace el trabajo del programador desconocido; a menudo destruye los datos, a veces se enmascara como otro programa existente en el sistema y otras crea identificadores de usuario y contraseñas.
- Actualizaciones y descargas. Algunas computadoras permiten la actualización del firmware y/o del sistema operativo a través de la red y muchas veces incluye código malicioso.

e) ***Puertas de Escape***. Conocidas también como puertas traseras, son introducidas en los sistemas operativos para permitir el acceso al sistema en el caso de que un cliente pierda toda la información de sus accesos autorizados. A veces las puertas traseras tienen como resultado errores en el sistema, lo que significa que nadie entiende como funcionan excepto la gente que los descubre e incluso ellos podrían no entender el proceso sino solamente el resultado. Las diversas amenazas contra la seguridad debido a las puertas traseras son:

- "Piggybacking". Hace referencia a una situación en la que un usuario termina la comunicación con otro sistema, pero por alguna razón, el puerto permanece activo en el otro sistema. Entonces, algún usuario puede empezar la comunicación con el otro sistema en el mismo puerto sin pasar ningún control de seguridad.
- Servicios no seguros. A veces, los servicios de un sistema operativo pueden evitar el sistema de seguridad propio de la máquina.
- Configuración e instalación. Es posible que al iniciar el sistema después de algún mantenimiento, los mecanismos de seguridad no se inicien correctamente, dejando agujeros de seguridad que pueden ser utilizados por otras personas.

4.3.5. Otros Impedimentos de la Seguridad

Adicionalmente existen otros impedimentos a la seguridad (Figura 4.5) relacionados con las políticas existentes en la organización y son:

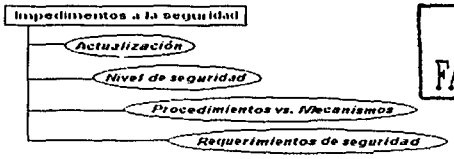


Figura 4.5: Impedimentos adicionales de la seguridad.

- Actualización. Para convertir un sistema actual en seguro, se debe enfrentar el problema de actualizar la seguridad en los componentes, mecanismos y entornos actuales. Como en el desarrollo de nuevos sistemas comienza a incorporarse algo de seguridad en las primeras fases del diseño y desarrollo de procesos, el problema de actualización de la seguridad ha comenzado a reducirse ampliamente.

- Nivel de Seguridad. "La evidencia de que un sistema es seguro se conoce como evidencia de seguridad; desafortunadamente, los únicos tipos de evidencia de seguridad que están disponibles incluyen los resultados de pruebas (que no pueden ser usados para mostrar la ausencia de problemas), resultados de campo (que no pueden evaluar todos los aspectos de un sistema de manera uniforme) y el uso de métodos formales (que no han demostrado gran éxito sobre sistemas grandes)"[5]. Así, proveer la adecuada evidencia de seguridad es generalmente una tarea difícil. La seguridad, sin embargo, no es fácilmente demostrable debido a que la mitigación de posibles ataques no conduce a demostraciones convincentes. Como resultado, la provisión de evidencia de seguridad es más importante para los sistemas seguros que para muchos tipos de aplicaciones.

[5] Amoroso, Edward. 1994. Ed. Prentice-Hall. "Fundamentals of Computer Security Technology".

- Procedimientos vs. Mecanismos. Los procedimientos y mecanismos son necesarios para reducir las amenazas de un sistema de cómputo; estos procedimientos y mecanismos varían desde políticas de administración del personal, recursos y operaciones hasta mecanismos funcionales diseñados en un sistema de cómputo. En algunos casos. proveer seguridad requiere una combinación de procedimientos y mecanismos; otras veces es suficiente con sencillas políticas de seguridad. Las organizaciones que deben proteger la información pueden decidir instalar mecanismos de seguridad funcionales dentro de su ambiente computacional. Adicionalmente se pueden instalar controles de acceso y configuración. mecanismos de autenticación y herramientas de auditoría en línea como un medio para establecer dicha protección.

- Requerimientos de Seguridad. La identificación de los requerimientos de seguridad es difícil para sistemas grandes y aun cuando los requerimientos han sido identificados, en la práctica, el desarrollo de sistemas que reúnan estos requerimientos es muy bajo.

4.4. Tipos de Vulnerabilidades y Ataques en Comunicaciones

El término genérico del campo que trata las herramientas diseñadas para proteger los datos y frustrar a los piratas informáticos es ***seguridad en computadoras***. Las medidas de ***seguridad en red*** son necesarias para proteger los datos durante su transmisión y garantizar que los datos transmitidos sean auténticos.

El problema de la seguridad en redes puede verse como un problema de seguridad computacional para una aplicación especifica, lo cual permite ver a la seguridad de las redes como la determinación de amenazas, vulnerabilidades y evaluación de ataques; definición de políticas, un modelo de seguridad y defensas, así como la instalación de medidas de seguridad a las aplicaciones de la red como si se aplicaran a los programas computacionales en general.

4.4.1. Vulnerabilidades Genéricas

"Las vulnerabilidades pretenden describir las debilidades y los métodos más comunes que se utilizan para perpetrar ataques a la seguridad de la familia de protocolos TCP/IP (confidencialidad, integridad y disponibilidad de la información)"[6].

Los ataques pueden ser motivados por diversos objetivos, incluyendo fraude, extorsión, robo de información confidencial, venganza, acceso no autorizado a un sistema, anulación de un servicio o simplemente el desafío de penetrar un sistema. Los ataques pueden provenir principalmente de dos fuentes:

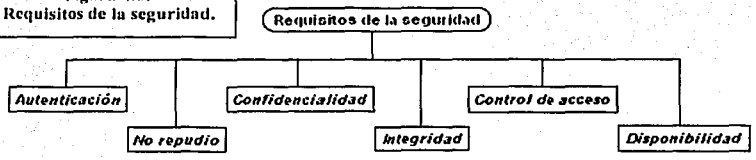
[6] Ídem.

1. Usuarios autentificados, al menos a una parte de la red, como por ejemplo empleados internos o colaboradores externos con acceso a sistemas dentro de la red de la empresa.
2. Atacantes externos a la ubicación física de la organización, los cuales pueden accesar remotamente a la red.

4.4.2. Requisitos de la Seguridad

Para ser capaz de entender los tipos de ataques existentes a la seguridad, es conveniente definir los requisitos de la seguridad (Figura 4.6). La seguridad de computadoras y redes implica los siguientes requisitos:

Figura 4.6: Requisitos de la seguridad.



1. Confidencialidad o Secreto. Sólo las personas o máquinas autorizadas pueden accesar a la información transmitida a través de una red de comunicaciones o al contenido de la información guardada en un sistema informático. En algunos casos no sólo hay que proteger el contenido de los mensajes (confidencialidad del mensaje), sino también las identidades del emisor y del receptor (confidencialidad del tráfico de mensajes). Este tipo de acceso incluye la impresión, desplegar en pantalla y otras formas de revelación que incluyen cualquier forma de dar a conocer la existencia de un objeto.
2. Integridad. Ninguna persona no autorizada puede modificar la información transmitida o almacenada. El mensaje debe llegar a su destino sin haber sufrido ninguna alteración en su contenido o en el orden de la recepción de sus unidades si se compone de varios bloques. La modificación incluye escribir, cambiar de estado, suprimir y crear.
3. Autenticación. El origen de un mensaje debe estar perfectamente identificado.
4. No repudio. Debe quedar constatado si un usuario envía o recibe algún mensaje, de esta manera, ni el emisor del mensaje ni el receptor del mismo pueden negar que se haya efectuado la transmisión.
5. Control de acceso. Sólo los usuarios autorizados debidamente identificados pueden obtener permiso de acceso a los recursos del sistema.
6. Disponibilidad. El sistema no debe permitir que usuarios no autorizados dejen fuera de funcionamiento elementos de la red impidiendo de esta manera las comunicaciones. Requiere que los recursos de una computadora estén disponibles sólo al personal autorizado.

La experiencia en la seguridad de redes ha conducido a los investigadores a creer que deben existir tres elementos primarios para proveer su seguridad:

1. Cifrado. El cifrado de la información que transita a través de la red es el elemento más estable y reconocido en la seguridad. Desafortunadamente, si el cifrado no se emplea en conjunto con los otros elementos, no será efectivo.
2. Protocolos. Los protocolos para autenticación y secreto en las redes de computadoras proveen un medio para organizar y proteger la comunicación de mensajes entre los componentes de la red. Deben ser usados en conjunto con los otros elementos de seguridad de la red.
3. Componentes confiables. Los componente confiables a menudo proveen el mejor medio para proteger la operación de aquellos mecanismos que hacen cumplir la seguridad de la red.

4.4.3. Evolución de los Ataques a la Seguridad

Los ataques a la seguridad se pueden clasificar en diferentes etapas como sigue:

- Primera generación: Ataque físico. Ataques que se centraban en los componentes electrónicos, es decir, computadoras y cables; el objetivo de los protocolos distribuidos y de la redundancia es la tolerancia frente a un punto único de fallo, la mayoría son problemas para los que actualmente se conoce una solución.
- Segunda generación: Ataque sintáctico. Las pasadas décadas se han caracterizado por ataques contra la lógica operativa de las computadoras y las redes, es decir, pretenden explotar las vulnerabilidades de los programas, de los algoritmos de cifrado y de los protocolos, así como permitir la negación del servicio prestado. En este caso se conoce el problema y se está trabajando para encontrar soluciones cada vez más eficaces.
- Tercera generación: Ataque semántico. Se basan en la manera en que los humanos asocian significado a un contenido; el hecho es que en la sociedad actual la gente tiende a creer todo lo que lee (medios informativos, libros, www - World Wide Web -). El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o e-mails; también pueden llevarse a cabo modificando información caduca. "Esta generación de ataques se lleva a su extremo si se modifica el contenido de los datos de los programas de la computadora que son incapaces de cotejar o sospechar su veracidad; dichos ataques han existido fuera del entorno informático desde hace muchos años. Su solución pasará no sólo por el análisis matemático y técnico, sino también por el humano"[7].

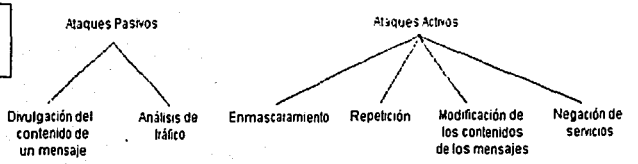
4.4.4. Clasificación de los Ataques

"Las ataques a la seguridad de red se dividen en dos categorías: ataques activos que suponen alguna modificación de los datos transmitidos o la creación de transmisiones falsas

[7] Ídem.

y ataques pasivos, llamados en ocasiones escuchas y suponen el intento de un atacante de obtener información relativa a una comunicación"[8](Figura 4.7). Adicionalmente existe un tipo de ataque que se enfoca principalmente a los medios de transmisión y a los dispositivos de red instalados en el sistema de comunicaciones

Figura 4.7: Clasificación de los ataques.



a) Ataques Activos

"Los ataques activos suponen una modificación del flujo de datos o la creación de flujos falsos y se subdividen en 4 categorías: enmascaramiento, repetición, modificación de mensajes y negación de un servicio"[9].

- Enmascaramiento o fabricación. Tiene lugar cuando una entidad pretende ser otra entidad diferente; un ataque de enmascaramiento normalmente incluye una de las otras formas de ataques activos. Por ejemplo, se puede captar una secuencia de autenticación y reemplazarla por otra secuencia de autenticación válida, habilitando a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.
- Repetición. Supone la captura pasiva de unidades de datos y su subsecuente retransmisión para producir un efecto no autorizado.
- Modificación de mensajes. Significa sencillamente que alguna porción del mensaje legítimo es alterada, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado.
- Negación de un servicio o interrupción. Previene o inhibe el uso o gestión normal de las facilidades de comunicación. Este ataque puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. Otro tipo de negación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de modo que se degrade su rendimiento.

Los ataques activos presentan características opuestas a los ataques pasivos. Mientras que un ataque pasivo es difícil de detectar, existen medidas disponibles para prevenirlos; por otro lado, es bastante difícil prevenir un ataque activo, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. En consecuencia, la meta es detectarlos y recuperarse de cualquier perturbación o retardo causado por ellos.

[8] Stallings, William. 2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".
[9] Ídem.

b) Ataques Pasivos

"Los ataques pasivos son del tipo de escuchas o monitoreo de las transmisiones; la meta del oponente es obtener información que está siendo transmitida. Existen tres tipos de agresiones: divulgación del contenido de un mensaje, análisis de tráfico e intercepción"[10].

- Divulgación del contenido del mensaje. Una conversación telefónica, un mensaje de correo electrónico o un archivo transferido puede contener información sensible o confidencial, por lo que sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.
- Análisis de tráfico. Cuando se tiene un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturen los mensajes, no se podrá extraer la información del mensaje, pero incluso si se cuenta con protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes, asimismo podría determinar la localización y la identidad de las computadoras que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se está realizando.
- Intercepción. Alguien no autorizado accede a cierta información o a cualquier elemento de la red.

Los ataques pasivos son muy difíciles de detectar ya que no implican la alteración de los datos, sin embargo es factible prevenir el éxito de estas agresiones. Por ello el énfasis para tratar estos ataques es la prevención antes que la detección.

c) Ataques a los Dispositivos de Comunicaciones

- Ataques a los medios de transmisión. El medio de transmisión utilizado para transportar la información entre los diferentes componentes de la red es susceptible a ciertos tipos de ataques. En particular, la intercepción de datos puede ser posible si se utilizan transmisiones de radio, líneas telefónicas o cualquier otro medio convencional. Un tipo de vulnerabilidad que se encuentra en algunos medios de transmisión es la radiación electromagnética que potencialmente puede ser modulada para enviar información o interceptada para obtener datos.
- Ataques a los módems. El uso de módems para accesar a los sistemas de cómputo introduce una clase de ataque basado en las características del módem y la configuración básica seleccionada por el usuario; la principal vulnerabilidad introducida cuando se utilizan módems es el acceso ilimitado a los datos y fuentes del sistema.
- Ataques a los switches y routers. Este tipo de ataques se refieren al hecho de que una persona no autorizada intenta accesar a estos dispositivos con el fin de alterar su configuración y en consecuencia el funcionamiento de la red.

[10] Ídem.

CAPÍTULO 5

Mecanismos de Protección de la Información

5.1. Introducción a la Criptología

5.1.1. Ramas de la Criptología

La criptología está formada por dos técnicas complementarias: *criptoanálisis* y *criptografía*.

Etimológicamente criptología quiere decir "escritura secreta", sin embargo, actualmente su significado es "la ciencia de la comunicación segura" cuyo objetivo es que dos partes puedan intercambiar información sin que una tercera parte no autorizada, a pesar de que capte los datos, sea capaz de descifrar la información.

La criptografía actúa mediante criptosistemas; "un criptosistema o sistema de cifrado es un sistema que permite cifrar los mensajes de tal forma que una persona no autorizada no pueda descifrar el mensaje, por lo que la criptografía se considera como la ciencia de diseñar criptosistemas. La criptografía es la técnica de convertir un texto inteligible, texto en claro (*plaintext*), en otro, llamado criptograma o texto cifrado (*ciphertext*), cuyo contenido de información es igual al anterior pero sólo lo pueden entender las personas autorizadas.

Por su parte el criptoanálisis es la técnica de descifrar un criptograma, sin tener la autorización, que trata de romper los cripotosistemas para apoderarse de la información cifrada"[1].

a) Criptografía

Para cifrar se debe transformar un texto mediante un método cuya función inversa únicamente conocen las personas autorizadas. Así, se puede utilizar un algoritmo secreto (Figura 5.1 (a)) o un algoritmo público que utiliza una palabra, llamada **clave**, sólo conocida por las personas autorizadas, esta clave debe ser imprescindible para el cifrado y descifrado (Figura 5.1 (b)).

[1] Varios Autores. 2001. Ed. Alfaomega. "Técnicas Criptográficas de Protección de Datos".

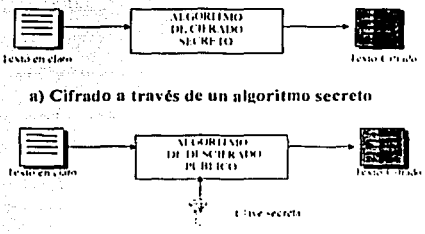


Figura 5.1: Proceso de cifrado / descifrado.

a) Cifrado a través de un algoritmo secreto

b) Descifrado mediante clave secreta

Los sistemas actuales utilizan algoritmo público y claves secretas, debido a los siguientes motivos:

- El nivel de seguridad es el mismo.
- Los algoritmos públicos se pueden fabricar en cadena, tanto en chips de *hardware* como en aplicaciones *software*. De está manera el desarrollo es más barato.
- Los algoritmos públicos están más probados, ya que toda la comunidad científica puede trabajar sobre ellos buscando fallas o agujeros. Un algoritmo secreto puede tener agujeros detectables sin necesidad de conocer su funcionamiento completo, por lo tanto, un criptoanalista puede encontrar fallas aunque no conozca el secreto del algoritmo.
- Es más fácil y más seguro transmitir una clave que todo el funcionamiento de un algoritmo.

De esta manera un sistema de comunicaciones con criptografía utiliza un algoritmo público para cifrar y otro para descifrar, pero son completamente inservibles para el criptoanalista sin el conocimiento de la clave (Figura 5.2).

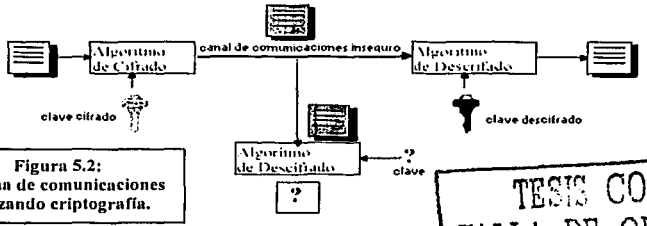


Figura 5.2: Sistema de comunicaciones utilizando criptografía.

b) Criptoanálisis

El criptoanálisis abarca diversas técnicas, las cuales muchas veces no dependen del conocimiento del algoritmo sino que mediante sistemas de aproximación matemática se

puede descubrir el texto en claro o la clave. La dificultad del análisis depende de la información disponible, así el criptoanalista puede tener acceso a:

- Un criptograma.
- Un criptograma y su texto en claro.
- Un texto claro elegido y su criptograma.
- Un criptograma elegido y su texto en claro.
- Un texto en claro y su criptograma que están previamente elegidos.

Aumenta la dificultad cuanto menos información se tiene, pero en todos se busca la clave que proporciona la solución para todo el sistema de seguridad.

En el criptoanálisis científico se utilizan las siguientes definiciones:

- Distancia unívoca. Cantidad mínima del mensaje para poder descifrar la clave. Un sistema ideal tiene una distancia unívoca de infinito.
- Sistema incondicionalmente seguro. El criptograma generado es menor que la distancia unívoca.
- Romper un sistema. Conseguir un método práctico para descifrar la clave de un sistema criptográfico.
- Sistema probablemente seguro. No se ha probado como romperlo.
- Sistema condicionalmente seguro. Los analistas potenciales no disponen de medios para romperlo.
- No existen los sistemas completamente seguros. Siempre se pueden violar probando todas las claves posibles. Por lo tanto, en criptografía se buscan sistemas que cumplan una de siguientes condiciones:

a) El *precio* para romperlo es más caro que el *valor* de la información.
b) El *tiempo* necesario para romperlo es más largo que el *tiempo de vida* de la información.

5.1.2. Evolución de la Criptografía

a) Método Julio Cesar

Es el más antiguo conocido. La época de Julio Cesar es la primera que se tiene noticia de la popularización de la escritura de un idioma, el latín, ya que éste tuvo una gran difusión entre diferentes ejércitos y clases sociales. Así apareció la necesidad de ocultar información escrita y, por lo tanto, de la criptología.

El sistema reemplaza cada letra por la situada tres posiciones delante en el alfabeto. Por ejemplo:

B ⇒ E
Y ⇒ A
LLEGUE VI VENCI ⇒ OOHJXH YL YHQFL

Es fácil de romper:
- Prueba y ensayo con 26 intentos.
- Métodos estadísticos.

b) Sistemas Monoalfabéticos

Sustituyen cada letra por otra que ocupa la misma posición en un alfabeto desordenado, de este modo se consiguen tantas claves como posibilidades de alfabetos hay: Nº de claves 26! = $4.03X10^{26}$

"Es mucho mejor que el método de Julio Cesar y tiene más claves que el sistema más utilizado actualmente DES (2^{56} = $7.20X10^{16}$ claves). No se puede utilizar prueba y ensayo para romperlo"[2].

El problema está en cómo recordar la clave, es decir, el alfabeto desordenado. Para ello se utiliza una palabra de uso común que permite crear, con un algoritmo conocido, el alfabeto desordenado. Entonces, en la práctica, las claves posibles no son los alfabetos sino que las palabras fáciles de recordar, muchas menos que 26!.

El sistema es el siguiente:

1. Se busca una palabra (clave) fácil de recordar y se le quitan las letras duplicadas.
   SEGURIDAD ⇒ SEGURIDA
2. Se añaden al final de la palabra las letras restantes del alfabeto.
   SEGURIDABCFH.....XYZ
3. Se ordenan en una matriz cuya primera fila es la palabra clave.

   S E G U R I D A
   B C F H J K L M
   N O P Q T V W X
   Y Z

4. El nuevo alfabeto se lee por columnas de abajo hacia arriba.
   YNBSZOCEPFGQHUTJRVKIWLDXMA

La clave es más fácil de transmitir y recordar, pero el sistema de prueba y ensayo se reduce a todas las palabras conocidas. El mejor sistema de criptoanálisis para romper el algoritmo es el estadístico.

c) Playfair

"Inventado por el británico Ser Charles Wheatstone en 1854. Es un sistema monoalfabético de diagramas (grupos de dos letras). Utiliza una palabra clave y una matriz de 5x5"[3].

[2] Idem.
[3] Idem.

Ejemplo:
CLAVE: SEGURIDAD ⇒ SEGURIDA

S	E	G	U	R
I/J	D	A	B	C
F	H	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

I/J comparten celda.

Método de cifrado:

1. Las palabras se separan en diagramas. Un diagrama nunca puede tener dos letras repetidas, en ese caso se pone una (X) de relleno.
   Ejemplo: LLAVE ⇒ LX LA VE

2. Si las dos letras están en la misma fila se reemplazan por la siguiente de la derecha, las filas tienen continuidad mediante un sistema circular.
   Ejemplo: ER ⇒ GS

3. Si las dos letras están en la misma columna se sustituyen por la inmediata inferior, siguiendo un sistema circular.
   Ejemplo: BY ⇒ LU

4. En los casos restantes se sustituye cada letra por la correspondiente de la misma fila y la columna de la otra letra del diagrama.
   Ejemplo: LE ⇒ HU

Ventajas:
- Utiliza diagramas, 26 x 26 = 676 símbolos.
- La identificación individual es muy difícil.
- Métodos estadísticos de criptoanálisis complicados.

Durante muchos años se consideró irrompible. Fue utilizado por la armada inglesa y de Estados Unidos en las dos guerras mundiales. En realidad el sistema mejora la estadística pero sigue pareciéndose al texto en claro, sobre todo, para las letras poco frecuentes. Por lo tanto, con computadoras poderosas se puede romper fácilmente.

d) Sistemas Polialfabéticos

Se utilizan para cambiar las estadísticas del criptograma. A cada letra le corresponde un alfabeto; pero, ¿qué alfabeto?. Un sistema ideal utilizaría como clave alfabetos aleatorios pero serían imposibles de recordar y transmitir. Por lo tanto se utiliza una palabra clave y una tabla de alfabetos.

El sistema más famoso es la tabla de **Vigenère** (1586), alquimista, matemático y criptólogo del siglo XVI. La tabla es la siguiente:

	a	b	c	.	.	.	x	y	z
a	A	B	C	.	.	.	X	Y	Z
b	B	C	D	.	.	.	Y	Z	A
c	C	D	E	.	.	.	Z	A	B
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
x	X	Y	Z	.	.	.	U	V	W
y	Y	Z	A	.	.	.	V	W	X
z	Z	A	B	.	.	.	W	X	Y

Los alfabetos forman las columnas y siempre empiezan por la letra de la cabecera.

Método:
1. Se busca una palabra clave fácil de recordar.
2. Se escribe la palabra debajo del texto en claro, repitiéndose tantas veces como sea necesario.
3. Cada letra del texto en claro se codifica con el alfabeto de la tabla marcado por la letra inferior, o sea, la letra de la clave que corresponde.

Ejemplo:

CLAVE: ADIOS

Texto en claro:	E	S	T	O	E	S	C	R	I	P	T	O	L	O	G	I	A
Clave:	A	D	I	O	S	A	D	I	O	S	A	D	I	O	S	A	D
Criptograma:	**E**	**V**	**B**	**C**	**W**	**S**	**F**	**Z**	**W**	**H**	**T**	**R**	**T**	**C**	**Y**	**I**	**D**

El sistema de criptoanálisis sigue los siguientes pasos:

1. Se busca en el criptograma repeticiones de letras. Las repeticiones suponen coincidencias de texto en claro y clave.
2. Si la frecuencia entre repeticiones es de n letras ⇒ n es múltiplo de la longitud de la clave.
3. Se considera el texto como n textos intercalados, cada uno es monoalfabético con el alfabeto de una letra de la clave y se analizan por técnicas estadísticas.

La defensa es utilizar una clave tan larga como el texto, pero no es práctico: cuesta tanto transmitir la clave como el texto.

e) Sistemas de Permutación

Desordenan caracteres, bits, etc. No se pueden analizar con métodos estadísticos, no cambian los símbolos sino su situación en el texto. Existen diferentes métodos para recordar la forma de desordenar mediante una clave. Un ejemplo es:

- *Método de las columnas*
  1. Se elige una palabra clave fácil de recordar. Ésta forma la primera fila de una matriz.
  2. Debajo se añade el texto recorriendo las filas de derecha a izquierda.
  3. Se cambian las columnas de posición, la nueva posición ordena las letras de la palabra clave en orden alfabético.
  4. El nuevo texto se escribe con las letras de las columnas de abajo a arriba.

Ejemplo:
CLAVE: ROSAL
TEXTO: ESTO ES CRIPTOLOGIA

R	O	S	A	L
E	S	T	O	E
S	C	R	I	P
T	O	L	O	G
I	A			

Ordenación: ROSAL ⇒ ALORS

A	L	O	R	S
O	E	S	E	T
I	P	C	S	R
O	G	O	T	L
		A	I	

Criptograma: OIO GPE AOCS ITSE LRT

Desventajas:
1. Una permutación es fácil de detectar porque la estadística se mantiene.
2. Las columnas mantienen su estructura, por lo tanto, la distancia entre letras se mantiene.

El método genérico de análisis es: anagramas múltiples.

f) Técnicas Combinadas

Los algoritmos simétricos actuales combinan sustitución y permutación. Shannon publicó en 1949 el artículo: ***Communication Theory of Secrecy Systems***, donde propone dos técnicas combinadas para vencer los ataques a la criptografía:

1. Confusión. Para hacer más compleja la relación clave-criptograma realizar *sustituciones*.
2. Difusión. Para vencer los métodos estadísticos realizar *permutaciones* de los símbolos.

De este artículo se esperaba una explosión de la criptología, pero no fue así, en realidad únicamente resumía y daba consistencia científica a los sistemas utilizados durante toda la historia de la criptología.

La revolución de la criptología llega en 1976 con el artículo de Diffie y Hellman sobre criptografía asimétrica.

5.1.3. Criptografía de Clave Secreta o Simétrica

Es el sistema de criptografía más antiguo. Se utiliza desde los tiempos de Julio Cesar hasta la actualidad. Se caracteriza por usar la misma clave para cifrar y descifrar (Figura 5.3).

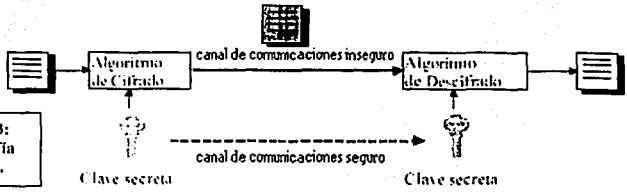


Figura 5.3: Criptografía simétrica.

"Toda la seguridad está basada en la privacidad de la clave secreta, llamada simétrica porque es la misma para el emisor y el receptor. El emisor del mensaje genera una clave y después la transmite mediante un canal seguro a todos los usuarios autorizados a recibir mensajes"[4]. La distribución de claves es un gran problema para los sistemas simétricos, hoy en día se resuelve mediante sistemas asimétricos montados únicamente para transmitir claves simétricas.

Estos sistemas sólo permiten confidencialidad y no autenticación ni firma digital. Para mantener la confidencialidad delante de un criptoanalista, el algoritmo debe cumplir las siguientes condiciones:

- Conocido el criptograma no se puede descifrar el texto ni adivinar la clave.
- Conocido el texto y el criptograma es más caro (en tiempo y/o dinero) descifrar la clave que el valor de la información.

Para la segunda condición siempre existe el sistema de "prueba y ensayo" para encontrar la clave, es decir, probar todas las claves posibles hasta encontrar la que descifra

[4] Idem.

el criptograma. La seguridad respecto a este tipo de ataque depende de la longitud de la clave.

Los algoritmos simétricos cifran bloques de texto, el tamaño de los bloques puede ser constante o variable según el tipo de algoritmo. Existen 4 formas de funcionamiento (Figura 5.4):

- ***Electronic CodeBook (ECB).*** Se cifran los bloques de texto por separado.
- ***Cipher Block Chaining (CBC).*** Los bloques del criptograma se relacionan entre ellos mediante funciones OR-EXCLUSIVA.
- ***Cipher FeedBack (CFB).*** Se realiza una OR-EXCLUSIVA entre caracteres o bits aislados del texto y las salidas del algoritmo. El algoritmo utiliza como entrada los criptogramas.
- ***Output FeedBack (OFB).*** Igual que el CFB, se realiza una OR-EXCLUSIVA entre caracteres o bits aislados del texto y las salidas del algoritmo. Pero éste utiliza como entradas sus propias salidas, por lo tanto no depende del texto, es un generador de números aleatorios.

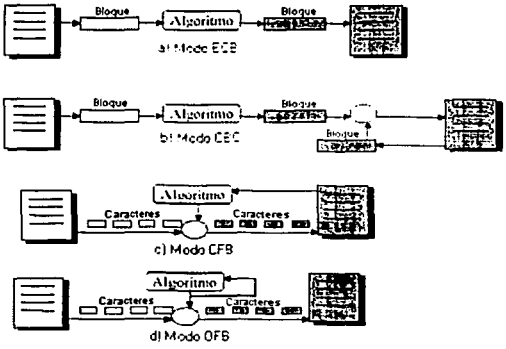


Figura 5.4: Formas de funcionamiento de los algoritmos simétricos.

Los algoritmos simétricos son más sencillos que los asimétricos, por ese motivo los procesos son más simples y rápidos. Los algoritmos más utilizados son:

- ***DES*** (Data Encryption Standard). El más utilizado y más antiguo, en 20 años nunca ha sido roto. Está sujeto a las leyes de seguridad de Estados Unidos.
- ***IDEA*** (International Data Encryption Algorithm). Se utiliza mucho en sistemas europeos nuevos. No está sujeto a las leyes de ningún país.
- ***RC5***. Algoritmo adoptado por *Netscape*, no está probada completamente su seguridad.

a) DES (Data Encryption Standard)

"En 1971 IBM inventó un algoritmo de cifrado simétrico basado en la aplicación de todas las teorías existentes sobre criptografía. Se llamó LUCIFER y funcionaba con claves simétricas de 128 bits. Fue vendido en exclusividad a la empresa de seguros Lloyd's"[5].

En 1973 el NBS (*National Bureau of Standards*) de los Estados Unidos convocó un concurso para elegir un estándar de cifrado para la seguridad de los documentos oficiales. Este concurso fue ganado en 1977 por los inventores del LUCIFER con una versión mejorada, este algoritmo se denominó DES (*Data Encryption Standard*). Desde entonces nunca ha sido roto.

Este algoritmo se ha mantenido como estándar del NIST (*National Institute of Standards and Technology*), agencia de estándares de Estados Unidos, hasta 1999. La versión implementada con *hardware* entró a formar parte de los estándares de la ISO con el nombre de DEA (*Data Encryption Algorithm*).

Inconvenientes del algoritmo:

1. Está considerado como secreto nacional en los Estados Unidos, por lo tanto, no se puede comercializar en *hardware* ni en *software* fuera de Estados Unidos sin permiso del Departamento de Estado. A pesar de esto, es el algoritmo más extendido del mundo.
2. La clave es corta, hasta ahora era suficiente para las máquinas existentes y un ataque de prueba y ensayo. Pero se considera que hoy en día o próximamente se podrá romper con máquinas potentes trabajando en paralelo a través de una red como Internet, por este motivo ya no es el estándar de seguridad de los Estados Unidos.
3. Hay un sistema matemático llamado criptoanálisis diferencial capaz de romper el DES en 2^{47} iteraciones si se conocen textos y criptogramas elegidos, es decir, si se tiene acceso al cifrador. Hoy en día no es un criptoanálisis práctico.

Ventajas del algoritmo:

1. Es el más extendido en el mundo, por lo tanto, es el que más máquinas utilizan (por ejemplo UNIX), más barato, más probado, etc.
2. En 20 años nunca ha sido roto con un sistema práctico.
3. Es muy rápido y fácil de implantar.

b) Triple DES (TDES)

Para evitar el problema de la clave corta y continuar utilizando el DES existe un sistema basado en tres iteraciones del algoritmo, llamado triple DES o TDES, que utiliza una clave de 128 bits y es compatible con el DES simple (Figura 5.5).

[5] Ídem.

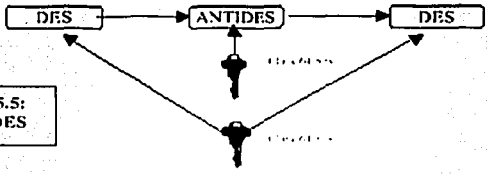


Figura 5.5: Triple DES

"Se utiliza una clave de 128 bits (16 de paridad y 112 de clave), se aplican 64 bits a los dos DES y los otros 64 bits al DES inverso (ANTIDES) que se realiza entre los otros dos"[6].

Con tres algoritmos se podrían aplicar tres claves distintas, pero no se hace así para que sea compatible con el DES. Si la clave de 128 está formada por dos claves iguales de 64 el sistema se comporta como un DES simple:

EK[DK[EK[Texto]]] = EK[Texto]

c) IDEA (International Data Encryption Algorithm)

"En 1990 *Lai* y *Massey* del *Swiss Federal Institute of Technology* inventaron un algoritmo nuevo denominado IDEA. En 1992 se publicó la segunda versión resistente a ataques de criptología diferencial. Este algoritmo está libre de restricciones y permisos nacionales y es de libre distribución por Internet. Esto ha hecho que sea un algoritmo muy popular, sobre todo fuera de los Estados Unidos, utilizándose en sistemas como: UNIX en Europa, PGP (Pretty Good Privacy) para correo electrónico, etc."[7]

Trabaja con bloques de texto de 64 bits y una clave de 128 bits. Puede funcionar con los 4 modos: ECB, CBC, CFB y OFB. Siempre opera con números de 16 bits utilizando operaciones como OR-EXCLUSIVA, suma de enteros o multiplicación de enteros. El algoritmo de descifrado es muy similar. Por estos motivos es sencillo de programar y rápido. Hasta ahora nunca ha sido roto, aunque no tiene la antigüedad del DES. Además su longitud de clave lo hace muy difícil de romper mediante "prueba y ensayo".

5.1.4. Criptografía de Clave Pública o Asimétrica

"En 1976 *Diffie* y *Hellman* publicaron el artículo "*New directions in cryptography*". En él proponían un nuevo tipo de criptografía basado en utilizar claves distintas para cifrar y descifrar, una de ellas se hace pública y la otra es privada de cada usuario. Así todos los usuarios de la red tienen acceso a las claves públicas, pero únicamente a su clave privada"[8]. Estas ideas supusieron la revolución de la criptología; se podía utilizar para confidencialidad (como los sistemas simétricos), autenticación y firma digital, además de

[6] Idem.
[7] Idem.
[8] Stallings, William.2000. Ed. Prentice-Hall. "Comunicaciones y Redes de Computadoras".

solucionar el problema de la distribución de claves simétricas. Para cada tipo de servicio se cifra de manera diferente:

- *Confidencialidad.* El emisor cifra el texto con la clave pública del receptor y el receptor lo descifra con su clave privada. Así cualquier persona puede enviar un mensaje cifrado, pero sólo el receptor, que tiene la clave privada, y el emisor, que lo ha creado, pueden descifrar el contenido (Figura 5.6).

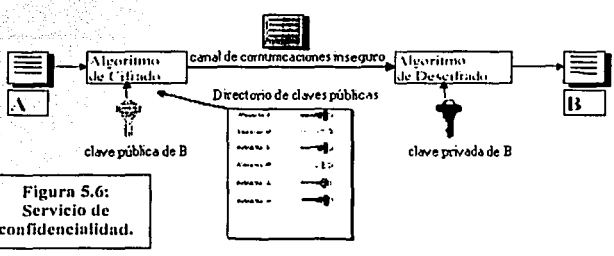


Figura 5.6: Servicio de confidencialidad.

- *Autenticación.* Se cifra el mensaje o un resumen de éste mediante la clave privada y cualquier persona puede comprobar su procedencia utilizando la clave pública del emisor. El mensaje es auténtico porque sólo el emisor verdadero puede cifrar con su clave privada (Figura 5.7).

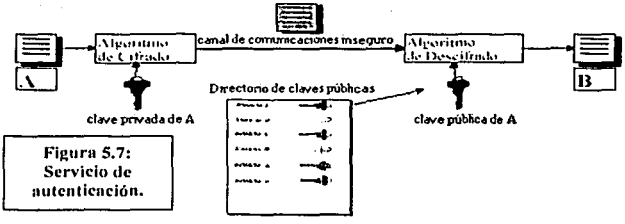


Figura 5.7: Servicio de autenticación.

- *Firma digital.* Igual que la autenticación, pero siempre se cifra el resumen del mensaje, cuyo criptograma es la firma del emisor. Así el emisor no puede negar la procedencia ya que se ha cifrado con su clave privada. Por otro lado, el receptor no puede modificar el contenido porque el resumen sería diferente y se vería que no coincide con la firma descifrada. Pero el receptor sí puede comprobar que el resumen coincide con la firma descifrada para ver si es auténtico (Figura 5.8). La firma digital lleva implícita la autenticación.

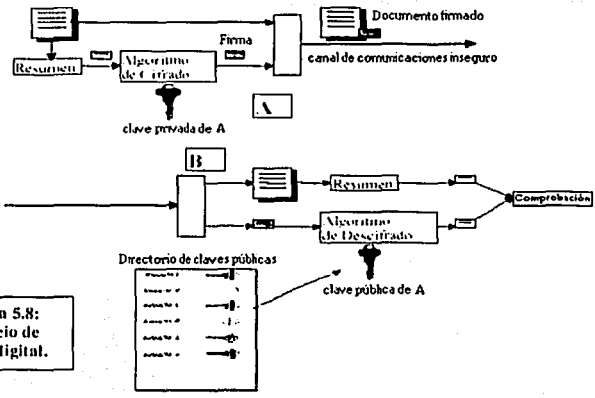


Figura 5.8: Servicio de firma digital.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver pero muy complicadas de realizar la inversa, por ejemplo, la potencia y el logaritmo.

Estas funciones son útiles para criptografía si la inversa es fácil de calcular conociendo un número concreto, la clave privada. Así la clave privada y pública están relacionadas matemáticamente, pero esta relación debe ser suficientemente compleja para que el criptoanalista no la pueda encontrar. Debido a esto, las claves privadas y públicas no las elige el usuario sino que las calcula un algoritmo y, normalmente, son muy largas.

Un algoritmo de clave pública debe cumplirlas siguientes condiciones:

- Conocido el criptograma no se puede descifrar el texto ni adivinar la clave.
- Conocido el texto y el criptograma es más caro (en tiempo y/o dinero) descifrar la clave que el valor de la información.
- Conocida la clave pública y el texto no se puede generar un criptograma cifrado con clave privada.

El inconveniente de estos sistemas es la dificultad de implantación y la lentitud de proceso.

La ventaja es que implantan servicios de autenticación y firma digital, y además no tienen problemas con distribución de claves: la clave pública puede ser visible por cualquiera y la privada no se transmite nunca.

El algoritmo más utilizado es el RSA (iniciales de sus creadores Rivest-Shamir-Adlman), es de libre circulación para claves de menos de 512 bits (insuficiente para ciertas aplicaciones). Únicamente para firma digital también se utiliza el algoritmo DSS (Digital

Signature Standard) que ha sido adoptado como estándar por el NIST. Para distribuir claves simétricas también se utiliza el algoritmo Diffie-Hellman, pero no sirve para confidencialidad, autenticación ni firma digital.

a) RSA (Rivest, Shamir and Adlman)

"Es el más popular y utilizado de los algoritmos asimétricos. Fue inventado en 1978 por Rivest, Shamir y Adlman que dan nombre al algoritmo. Patentaron el algoritmo y cuando alcanzó popularidad fundaron una empresa, RSA Data Security Inc., para la explotación comercial. Para su implantación y comercialización se deben pagar derechos a esta empresa, pero actualmente se encuentran muchas versiones gratuitas en Internet. Fuera de los Estados Unidos sólo está permita la utilización del algoritmo con claves menores o iguales a 512 bits"[9].

El algoritmo utiliza las siguientes claves:

- Como pública dos números grandes elegidos por un programa: **e** y **n**.
- Como privada un número grande **d**, consecuencia de los anteriores.

El cálculo de estas claves se realiza en secreto en la máquina depositaria de la privada. Este proceso tiene mucha importancia para la posterior seguridad del sistema. El proceso es el siguiente:

1. Se buscan dos número grandes (entre 100 y 300 dígitos) y primos: **p** y **q**.
2. Se calcula $\phi = (p - 1) * (q - 1)$ y $n = p * q$.
3. Se busca **e** como un número sin múltiplos comunes a ϕ.
4. Se calcula $d = e^{-1} \bmod \phi$. (mod = resto de la división de enteros).
5. Se hacen **públicas** las claves **n** y **e**, se guarda **d** como clave **privada** y se **destruyen p, q** y ϕ.

"Mediante "prueba y ensayo" es muy difícil calcular d ya que es un número de 512 bits o más. De esta manera el sistema de criptoanálisis utilizado es buscar la clave privada **d** a partir de las públicas **e** y **n**. Para esto basta con encontrar los números **p** y **q**, estos son la descomposición en factores primos de **n**, ya que $n = p * q$. No se ha descubierto aun ninguna forma analítica de descomponer números grandes en factores primos"[10].

Actualmente es aconsejable utilizar claves de 1024 bits. Está muy extendido como algoritmo asimétrico, es el más rápido y sencillo de los existentes. Tiene todas las ventajas de los sistemas asimétricos; los servicios de autenticación y firma digital sólo se pueden implementar con estos sistemas. Para confidencialidad se puede utilizar también clave simétrica (DES, IDEA, RC5, etc.) y estos son mucho más rápidos que el RSA. En la actualidad se utilizan sistemas mixtos simétricos para confidencialidad y asimétricos para distribución de claves simétricas, autenticación y firma digital.

[9] Ídem.
[10] Varios Autores. 2001. Ed. Alfaomega. "Técnicas Criptográficas de Protección de Datos".

5.1.5. Aplicaciones Criptográficas en Comunicaciones

Uno de los elementos clave de la seguridad de la red es el uso del cifrado para proteger el secreto y el origen de la transmisión de los datos entre diferentes componentes de la red. La aplicación más sencilla de cifrado en la red involucra el cifrado cuando se envía la información y el descifrado cuando se recibe en el destino final.

El enfoque más potente y más común en contra de los ataques a la seguridad de red es el cifrado; si se va a utilizar el cifrado para proteger la información que viaja a través de la red, entonces se necesita decidir qué es lo que se va a cifrar y dónde se va a colocar la máquina de cifrado. Existen 2 alternativas fundamentales: cifrado de enlace y cifrado extremo a extremo.

Supongamos que una computadora se conecta a una red de conmutación de paquetes X.25, establece un circuito virtual a otra computadora y se prepara para enviarle los datos utilizando un cifrado extremo a extremo. Los datos se transmiten por esa red en forma de paquetes, que constan de una cabecera y algunos datos de usuario, ¿qué parte de cada paquete cifrará la computadora?. Supongamos que la computadora cifra el paquete entero, incluyendo la cabecera. Esto no funcionará ya que sólo la otra computadora puede descifrar el paquete; el nodo de conmutación recibirá el paquete cifrado y no será capaz de leer la cabecera, por lo que no será capaz de encaminar el paquete. De lo anterior se concluye que la computadora sólo puede cifrar la parte de datos de usuario y no la parte de cabecera, para que ésta pueda ser leída por la red.

De este modo, con el cifrado extremo a extremo, los datos de usuario están seguros, sin embargo el modelo de tráfico no lo está, ya que las cabeceras de los paquetes se transmiten sin cifrarlas; para alcanzar un mayor grado de seguridad, se necesita cifrado de enlace y extremo a extremo.

"Cuando se utilizan ambas formas, la computadora cifra la parte de los datos del usuario usando una clave de cifrado extremo a extremo; después se cifra el paquete entero usando una clave de cifrado de enlace. Conforme el paquete viaja por la red, cada nodo conmutador descifra el paquete utilizando una clave de cifrado de enlace para poder leer la cabecera y luego cifra de nuevo el paquete entero para enviarlo al siguiente enlace. Ahora el paquete está seguro excepto durante el tiempo en el que el paquete está en la memoria del nodo de conmutación, en el que la cabecera está desprotegida"[11].

a) Cifrado Extremo a Extremo (End-To-End)

"En la técnica conocida como cifrado Extremo a extremo (End-To-End) (Figura 5.9), los mensajes son cifrados y descifrados como parte del procesamiento de las capas superiores; es decir, los mensajes son cifrados por el emisor y descifrados por el receptor en una capa superior a la capa utilizada para ruteo (capa 3) en un intermediario"[12].

[11] Amoroso, Edward. 1994. Ed. Prentice-Hall. "Fundamentals of Computer Security Technology".
[12] Idem.

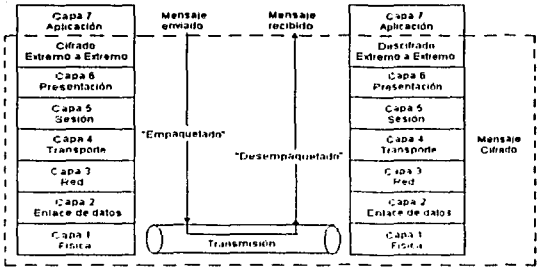


Figura: 5.9: Cifrado extremo a extremo (End-To-End).

La ventaja del método Extremo a extremo (End-To-End) es que el texto en claro solamente está disponible en el proceso de emisión y recepción, sin importar si los sistemas intermediarios manejan o no el mensaje como sea transmitido; esto es debido a que el cifrado se realiza en un nivel superior que el protocolo de ruteo.

Desafortunadamente, como tal método requiere que procesos de aplicación realicen el cifrado, se puede destruir la transparencia que se tiene con el cifrado de enlace; lo cual también impide el uso exclusivo de hardware para cifrado.

El proceso de cifrado se realiza en los dos extremos finales, la computadora o terminal origen cifra los datos, después los datos cifrados se transmiten sin alterarlos a través de la red hasta la computadora o terminal destino. El destino comparte una clave con el origen y por lo tanto es capaz de descifrar los datos; esta técnica protege la transmisión contra agresiones en los enlaces o conmutadores de red.

b) Cifrado de Enlace

Un método común que se emplea cuando un mensaje se envía directamente desde la máquina **A** a la máquina **B** que asegure de alguna manera el secreto y la autenticación es conocido como cifrado de enlace (Figura 5.10).

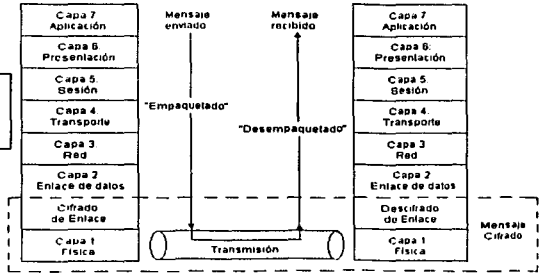


Figura 5.10: Cifrado de enlace.

En el método de cifrado de enlace, los mensajes enviados por una máquina son cifrados antes de que se coloquen en el medio físico para su transmisión a otra máquina.

Debido a que el cifrado de enlace se realiza en las dos primeras capas del modelo OSI, es transparente para las aplicaciones de las capas superiores. Además, puesto que el cifrado de enlace se realiza muy cerca del medio de transmisión, puede ser desarrollado por rutinas especializadas que operan rápida y eficientemente.

Sin embargo, existe un problema potencial si el cifrado de enlace se emplea en casos en los cuales se utiliza un intermediario para la transmisión entre las máquinas; es decir, si la máquina A envía un mensaje a la máquina B a través de un componente intermedio C (probablemente porque no existe una conexión directa entre A y B), entonces una versión en claro del mensaje transmitido puede estar disponible para leerse cuidadosamente en los componentes intermedios; esto puede ser aceptable si el intermediario está autorizado para tal proceso de lectura, pero generalmente no es así.

La razón de este problema es que los anuncios de ruteo entre los diferentes componentes generalmente se complementan incluyendo en el mensaje información de ruteo del protocolo de transmisión utilizado. Tal información de ruteo debe ser sustraída e interpretada por cualquier componente que sirva como intermediario entre el emisor y el receptor. Una vez que la información de ruteo ha sido obtenida, el mensaje puede ser enviado a través de otros intermediarios o al receptor final. Usualmente, este proceso no involucrará que el mensaje recibido llegue hasta la capa 7; sino que generalmente involucra solo un procesamiento en la capa 3.

"Cada enlace de comunicación vulnerable se equipa en ambos extremos con un dispositivo de cifrado, de este modo todo el tráfico a través de los enlaces de comunicaciones se protege aunque esto requiere muchos dispositivos de cifrado en redes grandes; otra desventaja es que el mensaje debe ser descifrado cada vez que entra un paquete en un conmutador debido a que éste debe leer la dirección (número de circuito virtual) en la cabecera del paquete para encaminarlo; de esta forma el mensaje es vulnerable en cada nodo. Si la red es de conmutación de paquetes pública, el usuario no tiene control sobre la seguridad en los nodos"[13].

5.2. Herramientas de Seguridad

Actualmente Internet es la principal vía para consultar y publicar información de una forma sencilla, económica y revolucionaria; del mismo modo, Internet ofrece la posibilidad de contaminar y destruir esta información. Por esta razón las empresas necesitan instrumentar medidas de seguridad para proteger sus datos y recursos en Internet. Existen diferentes enfoques para instrumentar dichas medidas, una de ellas es la seguridad de las redes de datos. A continuación se describen algunos métodos para implantar un sistema de seguridad en una red de datos.

[13] Ídem.

5.2.1. NAT (Network Address Translation)

a) Características

- Permite a una organización aparentar que su red utiliza direcciones IP diferentes a las que realmente usa.
- Convierte el espacio de direcciones IP no ruteables en direcciones ruteables.
- Se puede cambiar de ISP (Internet Service Provider) de una forma amigable.
- Está definido en el RFC (Request For Comments) 1631.

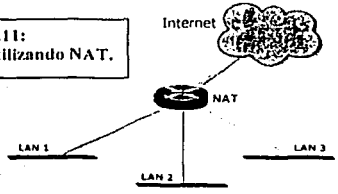
b) Posibles Usos de NAT

- Si se desea conectar a Internet, pero no se cuenta con un espacio de direcciones IP, se puede usar un direccionamiento privado. NAT se configura en el ruteador de frontera con el fin de crear una red interna y una externa (Internet). NAT traduce la dirección interna a una dirección global y única.
- Cuando se necesita cambiar el esquema de direccionamiento IP, el cual puede resultar caro y laborioso, se puede utilizar NAT para traducir al nuevo espacio de direcciones IP.

c) Posibles Esquemas

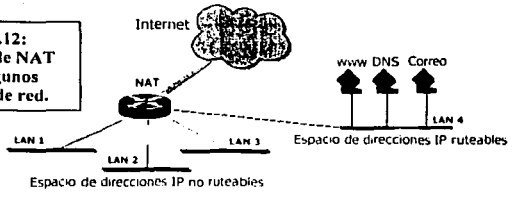
- Las direcciones de las LANs no son ruteables. A través de NAT se logra un acceso a Internet (Figura 5.11).

Figura 5.11:
Acceso a Internet utilizando NAT.



- La traslación puede ser aplicada sólo a algunos segmentos (LANs 1-3) sin afectar a los servidores que necesiten una dirección IP fija (Figura 5.12).

Figura 5.12:
Utilización de NAT solo en algunos segmentos de red.



d) Términos Relacionados

- Inside local address. La dirección IP asignada a un host en la red interna. La dirección es probablemente no legítima.
- Inside global address. Una dirección IP legítima que representa una o más *inside local IP address* para el mundo exterior.
- Outside local address. La dirección IP de un host externo como aparenta hacia la red interna.
- Outside global address. La dirección IP de un host asignada a este por el propietario del host.

e) Tipos de NAT

- Traslación Estática. Establece un mapeo uno-a-uno entre una dirección inside local y una dirección inside global. Es útil cuando un host debe ser accesible desde el exterior mediante una dirección fija.
- Traslación Dinámica. Establece un mapeo entre las direcciones inside local y un pool de direcciones globales.

f) Recomendaciones para el uso de NAT

- El direccionamiento privado debe basarse en el RFC 1918 para evitar el *overlapping*.
- NAT deberá tener como mínimo una interfaz interior y una exterior.
- Verificar que el espacio de direcciones IP demandado no sea mayor que el espacio IP global disponible.

El espacio privado de direcciones IP según el RFC 1918 es el siguiente:

- 10.0.0.0 - 10.255.255.255 – (prefijo 10/8, clase A)
- 172.16.0.0 - 172.31.255.255 – (prefijo 172.16/12, 16 clases B contiguas)
- 192.168.0.0 - 192.168.255.255 – (prefijo 192.168/16, 256 clases C contiguas)

5.2.2. Firewalls

"Un *firewall* es un dispositivo que permite a una red, tener conexión a Internet con cierto grado de seguridad. Existe una gran variedad de ataques o formas de violentar la seguridad de un sistema o red. Un firewall permite combatir diferentes tipos de ataques que son conocidos en Internet, entre ellos la intrusión, la negación de servicios y el robo de información"[14].

Un *firewall* generalmente se coloca en el punto donde la red interna se conecta a Internet o red externa (Figura 5.13).

[14] Gratton, Pierre. 1998. Ed. Trillas. "Protección Informática".

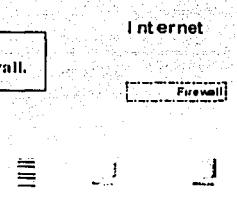


Figura 5.13:
Ubicación física de un firewall.

Al colocar el *firewall* de esta manera todo el tráfico que proviene o va hacia Internet pasa a través de él con lo cual el *firewall* tiene la capacidad de cerciorarse que el tráfico está de acuerdo con las políticas de seguridad del sistema. Estas políticas definen la accesibilidad y los niveles de restricción tanto de los servicios disponibles en Internet como los que se ofrecen en la red interna. Estas políticas son controladas a través de un solo punto central: el punto de conexión de la red con Internet.

Por ejemplo, un administrador de red podría definir como parte de las políticas para el tráfico de red, deshabilitar el servicio *telnet* desde Internet hacia la red interna y no utilizar servicios tales como NFS (Network File System) o NIS (Network Information Service) a través del *firewall*.

Puesto que todo el tráfico pasa a través del *firewall*, otra de las ventajas que presenta, es que éste se puede utilizar para recolectar información acerca de lo que ocurre entre la red protegida e Internet.

a) Definiciones Importantes

Para poder entender todos los conceptos relacionados con *firewalls*, es necesario conocer las siguientes definiciones:

- *Bastión.* Es un sistema de computación que debe ser altamente protegido, ya que es vulnerable a ataques, usualmente porque está expuesto a Internet.
- *Filtrado de Paquetes.* Es la acción que realiza un dispositivo para controlar selectivamente el flujo de datos que vienen desde y van hacia una red.
- *Red Perimetral.* Es una red que se encuentra entre la red protegida y la red interna con el objetivo de agregar una capa adicional de seguridad.
- *Servidor Proxy (gestor).* Es un programa que interactúa con servidores externos en nombre de clientes internos. Los clientes *proxy* se comunican con servidores *proxy* o sucedáneos que a su vez retransmiten las solicitudes legítimas a los servidores reales.

b) Tipos de Firewalls

El concepto de firewall puede efectuarse a través de:

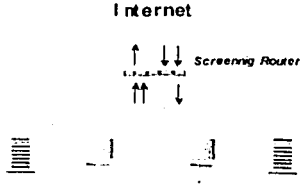
1. *Filtrado de paquetes.* Consiste en bloquear selectivamente el tráfico de red.
2. *Servidores proxy.* Se encargan de realizar la comunicación de red en lugar del cliente.

1. Filtrado de Paquetes

"Los sistemas de filtrado de paquetes direccionan los paquetes entre las máquinas de la red interna y externa, pero de forma selectiva dependiendo de las políticas que se tengan en el sistema. A este tipo de ruteadores que realizan filtrado de paquetes se les llama "*screening router*""[15].

Un *firewall* de filtrado de paquetes trabaja a nivel de paquetes; estos *firewalls* están diseñados para controlar el flujo de paquetes basándose en la dirección IP de origen y destino, los puertos de origen y destino e información del tipo del paquete. Adicionalmente, se puede controlar el flujo basándose en las interfaces de entrada o salida del paquete (Figura 5.14).

Figura 5.14: Filtrado de paquetes mediante un screening router.



Estos son algunos ejemplos para utilizar *firewalls* con filtrado de paquetes:

- Bloquear todas las conexiones desde sistemas externos a la red interna, excepto conexiones de correo vía SMTP (Simple Mail Transfer Protocol).
- Bloquear todas las conexiones desde una red externa en particular.
- Permitir los servicios telnet o FTP (File Transfer Protocol) desde la red interna, pero bloquear otros como RLOGIN (Remote Login), *RSH* (Remote Shell) *o TFTP* (Trivial File Transfer Protocol).

El filtrado de paquetes no toma decisiones basándose en el contenido en sí del paquete sino en el encabezado. Por esta razón no se pueden tomar acciones tales como las que se muestran en estos ejemplos:

- El usuario X puede hacer *telnet* a la red interna, pero el usuario Y no.

[15] Idem.

- Una persona puede transferir archivos tipo .wav pero no tipo .mp3.

En los ejemplos anteriores se pretende tomar decisiones basándose en cierto tipo de información que no pertenece al encabezado de los paquetes sino al contenido.

1.1. Reglas de Filtrado

Como se mencionó anteriormente, el filtrado de paquetes utiliza la siguiente información que poseen los paquetes para definir las reglas de filtrado:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto origen.
- Puerto destino.
- Protocolo.
- Tipo de paquete.

a) Filtrado por Dirección

"Esta es la forma más sencilla y más usada para realizar filtrado de paquetes. La restricción del flujo de paquetes se realiza basándose en la dirección origen y/o destino del paquete sin considerar qué protocolo está involucrado"[16]. Por ejemplo, si se desea bloquear todo el tráfico proveniente de la red 10.10.10.0/24:

Flujo	**Dirección Origen**	**Dirección Destino**	**Acción**
Entrante	10.10.10.0/24	-	Denegar

El signo "-" indica cualquier dirección destino. **Flujo** indica si el tráfico manejado por el ruteador es entrante o saliente. **Acción** indica qué hace el ruteador con el paquete. Generalmente existen tres acciones a tomar con un paquete de red:

1. *Aceptar.* Indica que este paquete pasó el criterio de filtrado y será reenviado tal como lo hace un ruteador cualquiera.
2. *Denegar.* Indica que este paquete no cumple con el criterio de aceptación y será descartado.
3. *Rechazar.* Indica que este paquete no cumple con el criterio de aceptación y será descartado, pero a diferencia de **Denegar**, se envía un mensaje ICMP (Internet Control Message Protocol) a la máquina origen informando lo ocurrido. Generalmente es un paquete ICMP de *destino inalcanzable* o *destino administrativamente inalcanzable*. De esta forma el que envía el paquete es avisado y no tratará de retransmitir de nuevo.

[16] Idem.

b) Filtrado por Servicio

Este es un tipo de filtrado más complejo y más completo ya que permite definir reglas basadas en servicios tales como *telnet*, SNMP (Simple Network Management Protocol), SMTP, etc. El software de filtrado utiliza la información de los puertos, protocolo y tipo que contiene cada paquete para realizar el filtrado por servicio. Por ejemplo, en el servicio *telnet* desde una máquina de la red interna 192.168.2.1 a una máquina en la red externa 10.10.10.1 (servicio saliente), los paquetes que van desde la máquina interna poseen la siguiente información (paquete saliente):

- Dirección origen: 192.168.2.1
- Dirección destino: 10.10.10.1
- Puerto origen: Un puerto aleatorio superior al 1023 (> 1023)
- Puerto destino: 23
- Protocolo: TCP
- Tipo de paquete: El primer paquete, el que establece la conexión, no tiene el bit ACK (Acknowledgment) activo, el resto sí lo tiene.

El bit ACK de los paquetes TCP permite identificar si se trata de un paquete de solicitud de conexión (donde el ACK no está activado) o si es otro de los paquetes de la conexión (donde sí está activado).

De la misma forma un paquete entrante de una conexión *telnet* posee la siguiente información:

- Dirección origen: 10.10.10.1
- Dirección destino: 192.168.2.1
- Puerto origen: 23
- Puerto destino: El mismo puerto que se utiliza como origen en un paquete saliente.
- Protocolo: TCP
- Tipo de paquete: De conexión, siempre tiene el bit ACK activo.

Con esta información se pueden construir las reglas de filtrado que permiten conexiones *telnet* salientes, pero nada más. Considerando la red externa como Internet y la red interna como 192.168.2.0/24:

Regla	Flujo	Dirección Origen	Dirección Destino	Protocolo	Puerto Origen	Puerto Destino	ACK	Acción
1	Saliente	192.168.2.0/24	-	TCP	>1023	23	-	Aceptar
2	Entrante	-	192.168.2.0/24	TCP	23	>1023	Si	Aceptar
3	Ambos	-	-	-	-	-	-	Denegar

La primera regla indica que se aceptan paquetes desde la red interna, a cualquier servidor *telnet* en Internet. La segunda regla indica que se aceptan paquetes de retorno desde el servidor *telnet* de Internet a la red interna. Dado que esta regla verifica que el bit

de ACK esté activado, se prohibe que se realicen conexiones entrantes desde el puerto 23 hacia cualquier puerto superior al 1024. La regla final indica que si el paquete no cumple con ninguna de las reglas anteriores, entonces es denegado.

Como ejemplo, a continuación se definen las reglas de filtrado para cumplir con la siguiente política en la red 192.168.1.0/24:

- Se permiten conexiones *telnet* salientes.
- Se permiten conexiones SMTP salientes.
- Se permiten conexiones SMTP entrantes al servidor de correos de la red. 192.168.1.1.
- Se permiten conexiones HTTP (Hypertext Transfer Protocol) salientes.
- Se permiten conexiones entrantes al servidor HTTP de la red. 192.168.1.2.

Regla	Flujo	Dirección Origen	Dirección Destino	Protocolo	Puerto Origen	Puerto Destino	ACK	Acción
1	Saliente	192.168.2.0/24	-	TCP	>1023	23	-	Aceptar
2	Entrante	-	192.168.2.0/24	TCP	23	>1023	Si	Aceptar
3	Saliente	192.168.2.0/24	-	TCP	>1023	25	-	Aceptar
4	Entrante	-	192.168.2.0/24	TCP	25	>1023	Si	Aceptar
5	Saliente	192.168.2.0/24	-	TCP	>1023	80	-	Aceptar
6	Entrante	-	192.168.2.0/24	TCP	80	>1023	Si	Aceptar
7	Entrante	-	192.168.1.1	TCP	>1023	25	-	Aceptar
8	Saliente	192.168.1.1	-	TCP	25	>1023	Si	Aceptar
9	Entrante	-	192.168.1.2	TCP	>1023	80	-	Aceptar
10	Saliente	192.168.1.1	-	TCP	80	>1023	Si	Aceptar
11	Ambos	-	-	-	-	-	-	Denegar

Las reglas 1 y 2 permiten realizar *telnet* desde cualquier máquina de la red interna. Las reglas 3 y 4 permiten enviar correo desde cualquier máquina de la red interna. Las reglas 5 y 6 permiten conectarse a servidores WWW desde cualquier máquina de la red interna. Las reglas 7 y 8 permiten que el servidor de correos reciba correos desde cualquier dirección de origen. Las reglas 9 y 10 permiten que cualquier máquina se pueda conectar al servidor WWW de la red interna. Por último la regla 11 bloquea cualquier otro tipo de paquete.

2. Servidores Proxy

"Los servicios *proxy* son aplicaciones especializadas que corren en una máquina *firewall*: ya sea en el ruteador de la red o en una máquina bastión, dichas aplicaciones toman los requerimientos de los clientes y los reenvían a los servidores verdaderos basándose en las políticas de seguridad del sistema"[17].

En un sistema que tiene un *firewall* con un servidor *proxy* (Figura 5.15), el servidor *proxy* evalúa las solicitudes de los clientes y decide si debe ser aprobada o denegada. Si la solicitud es aprobada el servidor *proxy* se comunica con el servidor real y le reenvía las

[17] Ídem.

solicitudes del cliente *proxy* al servidor y las respuestas del servidor real al cliente *proxy*. Por el contrario si es denegada, entonces la solicitud es descartada.

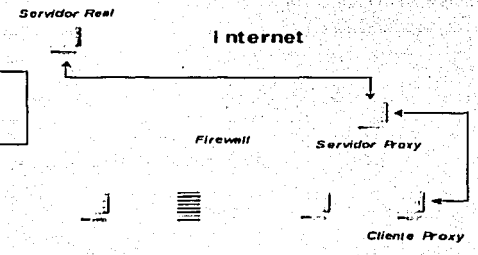


Figura 5.15: Firewall con un servidor proxy.

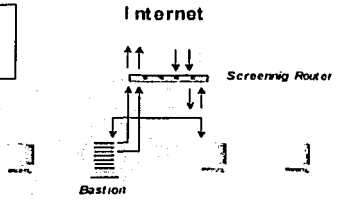
c) Arquitectura de Firewalls

A continuación se muestran las dos maneras más comunes de colocar los componentes de un firewall: *ruteador con filtrado de paquetes* y *firewall con red perimetral*.

1. Ruteador con Filtrado de Paquetes

En este tipo de *firewall*, el nivel primario de seguridad es provisto por el filtrado de paquetes (Figura 5.16). El bastión es la máquina que provee servicios tanto a la red interna como a la red externa. Por ejemplo, en el bastión puede estar el servidor WWW de la red interna, que puede ser consultado desde todo Internet. Adicionalmente, el bastión puede ser utilizado como servidor *proxy*.

Figura 5.16: Ruteador con filtrado de paquetes.



Todo intento de conexión a la red interna debe hacerse al bastión, por lo tanto, esta máquina debe mantener un alto grado de seguridad. La configuración del filtrado de paquetes en el ruteador puede realizarse de alguna de las siguientes formas:

- Permitir que otras máquinas de la red interna puedan conectarse a algunos de los servicios de Internet.

- Bloquear todas las conexiones de las máquinas internas a Internet. Todos los servicios deben ser solicitados al bastión configurado como servidor *proxy*.

Estos dos enfoques se pueden combinar en la configuración del *firewall*. Se pueden permitir algunas conexiones directamente a Internet, mientras que otras deben ser permitidas solo a través del servidor *proxy*.

Existen algunas desventajas en la utilización de esta arquitectura. La mayor de ellas es que si se rompe la seguridad del bastión, no hay nada que proteja al resto de la red interna. Además, el ruteador es un único punto de falla, si la seguridad de este dispositivo se ve comprometida, entonces el resto de la red queda expuesta a los ataques.

2. Red Perimetral

Esta arquitectura trata de evitar los problemas que existen con el ruteador de filtrado agregando una capa extra de seguridad, en donde se coloca una red perimetral que aísla la red interna de Internet.

Por su naturaleza, el bastión es la máquina más vulnerable de la red, debido a que esta máquina es la que permite la conexión directa desde Internet y posee servicios que pueden ser vulnerables. Para protegerlo, se aísla el bastión en la red perimetral, lo cual reduce el impacto de un ataque exitoso contra el bastión (Figura 5.17).

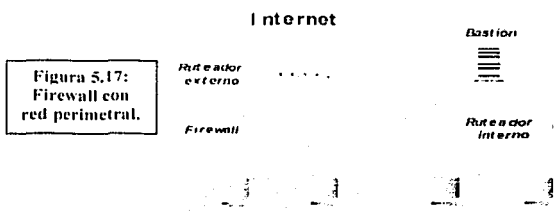


Figura 5.17: Firewall con red perimetral.

5.2.3. Filtros en los Dispositivos de Comunicaciones

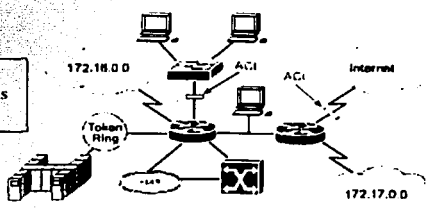
a) Listas de Accceso en Equipos de Ruteo

"Las ACL (Access Control List) son listas de instrucciones que se aplican a una interfaz del router. Estas listas indican al equipo qué tipo de paquetes se deben aceptar y cuales se deben denegar"[18] (Figura 5.18). La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y número de puerto. Las ACL permiten administrar el tráfico y examinar paquetes específicos, aplicando la ACL a

[18] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Segundo Año".

una interfaz del router. Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL.

Figura 5.18: Filtrado de paquetes a través de ACL.



Las ACL se pueden crear para todos los protocolos ruteables de red, como IP (Internet Protocol) e IPX (Internetwork Packet Exchange), para filtrar los paquetes a medida que pasan por un router. Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.

Las ACL filtran el tráfico de red en las interfaces del router controlando si los paquetes ruteados se envían o se bloquean. El router examina cada paquete para determinar si se debe enviar o descartar según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la dirección origen o destino del tráfico, el protocolo de capa superior, u otra información.

Las ACL se deben definir por protocolo. En otras palabras, es necesario definir una ACL para cada protocolo habilitado en una interfaz si se desea controlar el flujo de tráfico para esa interfaz. Por ejemplo, si la interfaz de router estuviera configurada para IP, AppleTalk e IPX, sería necesario definir por lo menos tres ACL. Las ACL se pueden utilizar como herramientas para el control de redes agregando la flexibilidad necesaria para filtrar los paquetes que fluyen hacia adentro y hacia afuera de las interfaces del router.

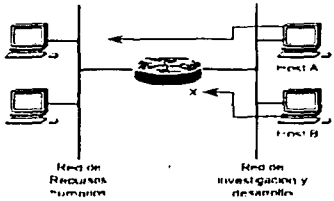
b) Usos de las ACL (Access Control List)

- Limitar el tráfico de red y mejorar el desempeño de la misma. Por ejemplo, las ACL pueden designar ciertos paquetes para que un router los procese antes de procesar otro tipo de tráfico, según el protocolo. Esto se denomina colocación en cola, que asegura que los routers no procesarán paquetes que no son necesarios. Como resultado, la colocación en cola limita el tráfico de red y reduce la congestión (Figura 5.19).
- Brindar control de flujo de tráfico. Por ejemplo, las ACL pueden restringir o reducir el contenido de las actualizaciones de ruteo. Estas restricciones se usan para limitar la propagación de la información acerca de redes específicas por toda la red.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host accese a una parte de la red y evitar que otro accese a la misma área. Al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red. Si no se

configuran ACL en el router, todos los paquetes que pasan a través de él tendrían acceso permitido a todas las partes de la red.

- Determinar el tipo de tráfico que se envía o bloquea en las interfaces del router. Por ejemplo, se puede permitir direccionar el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de telnet.

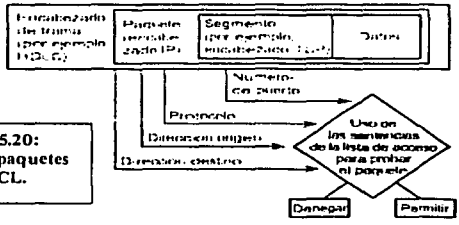
Figura 5.19: Uso de una ACL para limitar el tráfico de la red.



c) Prueba de Paquetes con ACL

En el caso de los ruteadores Cisco, el orden en el que se ubican las sentencias de la ACL es importante. Cuando el router está decidiendo si desea enviar o bloquear un paquete, el sistema operativo del dispositivo prueba el paquete verificando si cumple o no cada sentencia de condición en el orden en que se crearon las sentencias. Una vez que se verifica que existe una coincidencia, no se verifican otras sentencias de condición (Figura 5.20).

Figura 5.20: Prueba de paquetes con ACL.



Si se crea una sentencia de condición que permita todo el tráfico, no se verificará ninguna sentencia agregada más adelante.

Se puede crear una ACL por cada protocolo que se desea filtrar en cada interfaz del router. Para algunos protocolos, se crea una ACL para filtrar el tráfico entrante, y otra para filtrar el tráfico saliente.

Después de que una sentencia de ACL revisa un paquete para verificar si existe coincidencia, al paquete se le puede negar o permitir el uso de una interfaz en el grupo de acceso.

d) Características

Una ACL es un grupo de sentencias que define cómo los paquetes:

- Ingresan a las interfaces entrantes.
- Se direccionan a través del router.
- Se envían hacía las interfaces salientes del router.

"El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. Cuando un paquete entra en una interfaz, el router verifica si el paquete es ruteable o switching (puenteable); después, el router verifica si la interfaz entrante tiene una ACL. Si existe, se verifica que el paquete cumpla con las condiciones de la lista. Si el paquete es permitido, entonces se compara con las entradas de la tabla de ruteo para determinar la interfaz destino. Por último, el router verifica si la interfaz destino tiene una ACL. Si no la tiene, el paquete puede ser enviado directamente a dicha interfaz"[19] (Figura 5.21).

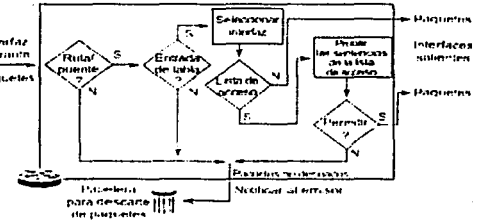


Figura 5.21: Secuencia de verificación de los paquetes de datos.

Las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si las sentencias de la ACL no se verifican, se impone una sentencia implícita de "denegar cualquiera"; esto significa que, aunque la sentencia "denegar cualquiera" no se vea explícitamente en la última línea de una ACL, está ahí.

1. Diagrama de Flujo del Proceso de Comparación de una ACL

Cuando la primera prueba indica que cumple la condición de negación, a un paquete se le deniega el acceso al destino. Se descarta y se elimina en la papelera de bits y no se expone a ninguna de las pruebas siguientes de la ACL. Si el paquete no concuerda con las condiciones de la primera prueba, pasa a la siguiente sentencia de la ACL. Las ACL permiten controlar lo que los clientes pueden accesar en la red (Figura 5.22). Las condiciones en un archivo de ACL pueden:

- Examinar ciertos hosts para permitir o negar el acceso a parte de su red.

[19] Idem.

- Configurar la autenticación de la contraseña, de manera que sólo los usuarios que proporcionan un identificador de conexión y una contraseña válidos pueden acceder a una parte de la red.
- Otorgar permiso a los usuarios para accesar a una parte de la red para utilizar los archivos o carpetas de un usuario en particular.

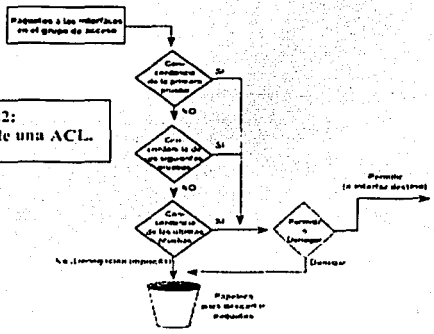


Figura 5.22:
Diagrama de flujo de una ACL.

2. Agrupación de ACL en Interfaces

"Aunque cada protocolo tiene su propio conjunto de tareas específicas y reglas que se requieren para proporcionar filtrado de tráfico, en general la mayoría de los protocolos requieren dos pasos básicos. El primer paso es crear una definición de ACL, y el segundo es aplicar la ACL a una interfaz"[20].

Las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente según la configuración. Las ACL salientes son generalmente más eficientes que las entrantes, y por lo tanto siempre se prefieren. Un router con una ACL entrante debe verificar cada paquete para ver si cumple con la condición de la ACL antes de conmutar el paquete a una interfaz saliente.

e) Tipos de ACL

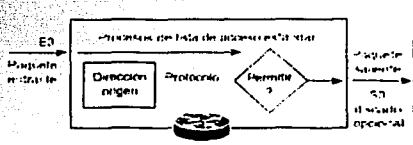
1. ACL Estándar

"Se deben usar las ACL estándar cuando se desea bloquear todo el tráfico de una red, permitir todo el tráfico desde una red específica o negar un conjunto de protocolos. Las ACL estándar verifican la dirección origen de los paquetes que se deben direccionar. El resultado permite o niega el acceso para todo un conjunto de protocolos, según las direcciones de red, subred y host"[21]. Por ejemplo, se verifican los paquetes que vienen de

[20] Ídem.
[21] Ídem.

E0 para establecer la dirección origen y el protocolo. Si se permiten, los paquetes salen a través de **S0**, que se agrupa en la ACL. Si no se permite, se descarta (Figura 5.23).

Figura 5.23: ACL estándar.



- **Especificaciones de direcciones más simples.**
- **Permite o deniega un conjunto de protocolos completo.**

2. ACL Extendida

"Las ACL extendidas se usan con mayor frecuencia para verificar condiciones porque ofrecen una mayor cantidad de opciones de control que las ACL estándar. Se puede usar una ACL extendida cuando se desea permitir el tráfico de la WWW pero negar el servicio de FTP o telnet desde las redes que no pertenecen a la empresa. Las ACL extendidas verifican las direcciones origen y destino de los paquetes; también pueden verificar protocolos, números de puerto y otros parámetros específicos, lo cual ofrece mayor flexibilidad para describir las verificaciones que debe realizar la ACL"[22]. Se pueden permitir o denegar paquetes según su origen o destino. Por ejemplo, la ACL extendida puede permitir el tráfico de correo electrónico desde **E0** a destinos **S0** específicos, denegando al mismo tiempo conexiones remotas o transferencias de archivos (Figura 5.24).

- **Especificaciones de direcciones más complejas.**
- **Permite o deniega protocolos específicos.**

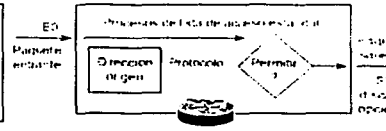


Figura 5.24: ACL extendida.

De acuerdo con el resultado de las pruebas realizadas por la ACL extendida, un paquete se puede permitir o denegar. Para las listas entrantes, significa que los paquetes permitidos seguirán siendo procesados; para las listas salientes, significa que los paquetes permitidos se enviarán directamente a la interfaz correspondiente. Si el resultado de las pruebas deniega el permiso, se descarta el paquete. La ACL del router suministra control de firewall para negar el uso de la interfaz en cuestión. Cuando se descartan paquetes, algunos protocolos devuelven un paquete al emisor indicando que el destino es inalcanzable.

Para una sola ACL, se pueden definir múltiples sentencias. Cada una de estas sentencias debe hacer referencia al mismo nombre o número de identificación, con el fin de relacionar las sentencias a la misma ACL. Se puede establecer cualquier cantidad de sentencias condicionales, con la única limitación de la memoria disponible en el equipo. Por cierto, cuanto más sentencias se establezcan, mayor será la dificultad para comprender y administrar la ACL. Por lo tanto, la documentación de las ACL evita la confusión.

[22] Idem.

Para un control más preciso de filtrado de tráfico se usan las ACL extendidas. Las sentencias de las ACL extendidas verifican la dirección origen y destino. Además, al final de la sentencia de la ACL extendida, se obtiene precisión adicional con un campo que especifica el número de puerto de protocolo opcional TCP o UDP, los cuales pueden ser números de puerto conocidos para TCP/IP. Algunos de los números de puerto más comunes aparecen en la tabla 5.1. Se puede especificar la operación lógica que la ACL extendida efectuará en protocolos específicos.

Tabla 5.1: Números de Puerto más Comunes.

Número de Puerto (Decimal)	Protocolo IP
20	Datos FTP (File Transfer Protocol)
21	Programa FTP (File Transfer Protocol)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
69	TFTP (Trivial File Transfer Protocol)
53	DNS (Domain Name Server)

f) Uso de las ACL en Routers Firewall

"Se deben utilizar ACL en routers firewall, que a menudo se colocan entre la red interna y una red externa, como Internet. El router firewall proporciona un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada. También se pueden usar las ACL en un router colocado entre dos partes de la red a fin de controlar el tráfico que entra o sale de una parte específica de la red interna"[23].

Para aprovechar las ventajas de seguridad de las ACL, como mínimo se deben configurar las ACL en los routers de frontera, los cuales están situados en el límite de la red interna y externa, lo que proporciona protección básica con respecto a la red externa, u otra parte menos controlada de la red, para acceder a un área más privada de la red. En estos routers de frontera, las ACL se pueden crear para cada protocolo de red configurado en las interfaces del router. Se pueden configurar las ACL para que el tráfico entrante, el tráfico saliente, o ambos, se filtren en una interfaz (Figura 5.25).

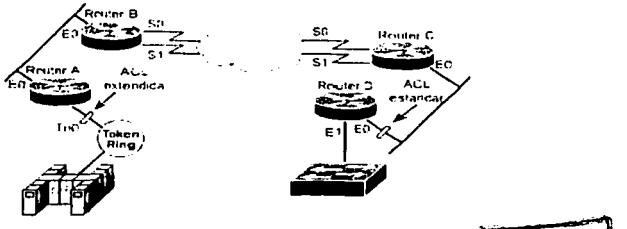


Figura 5.25: Ubicación de las ACL.

[23] Idem.

CAPÍTULO 6

Esquema Seguro para la Transmisión de Información

6.1. Objetivo

El propósito de este capítulo final es brindar las bases para el *análisis, diseño e implantación de un sistema de comunicaciones de datos con los mecanismos de seguridad necesarios* que permitan proteger la información que viajará a través de la red empresarial.

En primer lugar se puntualizan los *elementos* que se deben considerar al momento de escoger el medio de transmisión que se utilizará en la red empresarial, así como los *factores* que afectan el diseño de la misma y cómo deben ser interpretados por el diseñador de la red, con el fin de contar con los elementos suficientes para elaborar un buen diseño conceptual.

Asimismo se describe el uso de los *modelos jerárquicos* como la mejor opción para la implantación de la red, ya que al dividir la red en pequeñas células, resulta más fácil identificar los posibles puntos de falla del sistema de comunicaciones y corregirlos rápidamente sin afectar el desempeño global de la red.

Además se mencionan algunas *recomendaciones de seguridad* que pueden ser implantadas a través de políticas de seguridad o bien por medio de los equipos de cómputo y/o de comunicaciones, con el fin de proveer la seguridad adecuada a la red empresarial.

Finalmente se establece un *proceso* a través del cual se puede comprobar que efectivamente la red cubre los requisitos mínimos de seguridad establecidos por la organización, con lo que se asegura que los mecanismos de protección seleccionados cumplen con su objetivo primordial de mantener la *integridad y confiabilidad de la información* que circula por la red empresarial.

6.2. Determinación del Medio de Transmisión

El medio físico de transmisión es uno de los componentes más importantes que se debe tener en cuenta al diseñar una red. Los temas de diseño incluyen el tipo de medio que se debe utilizar y la estructura general del mismo.

Además de las limitaciones debidas a la distancia, se deben evaluar cuidadosamente las ventajas y las desventajas de las diversas topologías, ya que es del medio físico que depende la efectividad de la red. Se debe tomar en cuenta que la mayoría de los problemas de la red se deben a cuestiones de la capa 1 del modelo OSI. Si se planea hacer cambios significativos en una red, se debe realizar una auditoria completa del medio de transmisión para identificar las áreas que se deben actualizar y en las que se debe modificar la infraestructura física.

"La actualización del medio de transmisión debe tener prioridad sobre cualquiera de los demás cambios necesarios y las empresas deben asegurar (sin excepción) que estos sistemas cumplan con los estándares industriales bien definidos"[1].

6.2.1. Selección del Medio de Transmisión

"Son muchos los factores que influyen en la decisión de la selección del medio adecuado para la transmisión de datos, dichos factores incluyen costo, velocidad, crecimiento, seguridad y requerimientos en cuanto a la distancia"[2]; sin embargo estos factores no pueden considerarse de forma independiente, ya que la decisión del esquema apropiado depende del hardware que se tenga o se planea adquirir, asimismo los requerimientos de software pueden influir en la decisión final y en ocasiones se tendrá que reconfigurar el hardware para que funcione adecuadamente.

Además los diseñadores de sistemas de comunicación de datos tienen que tomar en cuenta dos tipos de diseños, uno para la comunicación entre el edificio o el campus, y otro para las comunicaciones remotas o de larga distancia.

a) Costo

El costo de una red de comunicaciones incluye no solo el costo del medio físico, sino que incluye el soporte de hardware y software requerido para la administración de la red; estos factores son únicamente el comienzo del proceso de mantenimiento. Muchos administradores señalan que el costo de la instalación del medio de transmisión es la pieza más grande del costo total del sistema de comunicaciones de datos, sin embargo la mayor parte del costo es, de hecho, el personal requerido para mantener el sistema. La experiencia requerida para mantener un sistema se incrementará conforme al tamaño del sistema; además, el costo de una futura expansión de debe tomar en consideración.

La comparación del costo utilizada en el diseño y selección del sistema de comunicaciones de datos debe tomar en cuenta el tiempo de vida del sistema y debe incluir al menos los siguientes elementos:

- El costo del medio de transmisión.
- El costo de instalación del medio de transmisión y todo el equipo de comunicaciones y procesamiento de datos necesarios para mantener el sistema.

[1] Servin, Claude.1999. Ed. Springer. "Telecommunications: Transmission and Network Architecture".
[2] Ramos, Emilio y Schroeder, Al. 1994. Ed. Macmillan. "Concepts of data Communications".

- El costo del personal necesario para el mantenimiento del sistema.
- El costo del personal que entrenará a los usuarios a utilizar el sistema.
- El costo de las actualizaciones o adiciones conforme a las necesidades de la compañía y el crecimiento de los usuarios.
- El costo del hardware y actualizaciones de software requeridas para mantener al sistema en operación.
- El costo de todos los enlaces contratados con los ISP's (proveedores de Internet).

b) Velocidad

La velocidad de transmisión del sistema de comunicación de datos se encuentra entre menos de 300 bits por segundo hasta varios millones de bits por segundo. El costo del incremento en la velocidad debe estar balanceado contra las necesidades del sistema de comunicación de datos y sus usuarios.

"Existen dos factores que influyen en la velocidad del medio de transmisión de datos: el tiempo de respuesta esperado por los usuarios y la tasa global de transmisión de datos. El tiempo de respuesta es el tiempo desde el momento en que una terminal envía una solicitud hasta el momento en que se recibe una respuesta que un host regresa al usuario; un buen tiempo de respuesta se considera entre 2 segundos o menos de 2 segundos. Sin embargo, se pueden tolerar tiempos de respuesta mayores para sustentar un menor costo del medio de transmisión. Típicamente es mejor tener un tiempo de respuesta lento y constante que un tiempo de respuesta impredecible.

La tasa global de transmisión de datos es la cantidad de información que puede ser transmitida por unidad de tiempo; los usuarios de una compañía estarán satisfechos con una velocidad de transmisión de 9600 bits por segundo, sin embargo en horarios pico, cuando el flujo de información es mayor, los requerimientos de velocidad pueden incrementarse alrededor de 19,200 bits por segundo o más"[3].

La fase de planeación durante la cual se diseña el sistema de comunicación de datos debe tomar en cuenta la carga en horas pico con el fin de tener un tiempo de respuesta predecible para los usuarios.

Adicionalmente, deben tomarse en cuenta los requerimientos futuros del sistema, ya que los avances tecnológicos se incrementan constantemente.

c) Crecimiento

Eventualmente, la mayoría de los sistemas de comunicación de datos necesitan extenderse agregando más dispositivos en alguna parte de la red o agregando nuevas sucursales.

[3] Idem.

En una situación donde la mayor cantidad del flujo de datos constantemente debe fluir entre dos sucursales remotas, contratar una línea puede no ser la mejor solución. Las microondas y otras tecnologías deberán ser consideradas y su costo debe ser comparado en relación a la vida útil de los sistemas, lo cual proveerá una idea más apropiada del costo actual y no solamente teniendo en cuenta el costo inicial de implantación del sistema de comunicación de datos.

El crecimiento futuro debe ser considerado desde el diseño de la red. Al momento de la planeación de los sistemas de comunicación debe considerarse el corto y el largo plazo, lo cual enfatiza la importancia de la planeación en estos sistemas.

La planeación debe incluir soluciones no solamente para las necesidades inmediatas de la organización (metas a corto plazo), sino que también debe anticipar las necesidades futuras más allá de 3 años (metas a largo plazo). Adicionalmente, el proceso de planeación debe hacerse de acuerdo a algún tipo de ciclo de vida que asegure que todos los aspectos del proceso de planeación han sido tomados en consideración adecuadamente para que el proyecto tenga éxito.

d) Seguridad

La falta de seguridad en una red de comunicación de datos permitirá que los hackers o personas no autorizadas tengan acceso a datos vitales de la organización, estos datos pueden ser usados para obtener ventajas en el mercado, o bien pueden ser alterados o destruidos provocando serias consecuencias para el negocio.

Proveer una red completamente cerrada, en la cual las personas no autorizadas en ningún momento tengan acceso la red es imposible. Sin embargo, algunos medios de transmisión, como la fibra óptica, son más difíciles de penetrar que otros medios, como el cable coaxial o la transmisión vía satélite. Los medios más vulnerables para un hacker ordinario son las líneas switcheadas. Una vez que una persona tiene acceso al equipo de switcheo, esta persona tiene acceso al resto de la red; el acceso al equipo de switcheo debe restringirse por medio de cuentas individuales de autenticación, passwords seguros o algún otro mecanismo que cuente con las medidas de autenticación adecuadas.

Otro tipo de amenaza en la seguridad es el ataque al sistema realizado por un virus de computadora; el cual puede ser introducido en el sistema de comunicación de datos por un empleado de la compañía. Una vez dentro del sistema, el virus puede expandirse y puede destruir los datos en las computadoras de los usuarios o en los equipos de cómputo principales donde se almacena la información crítica de la empresa. Para proteger los sistemas de comunicación de esta amenaza, pueden utilizarse antivirus o buscadores de virus para verificar cualquier disco utilizado en cualquier equipo de cómputo, o para verificar cualquier archivo que viaja a través de la red. Puede utilizarse algún software de monitoreo para alertar el administrador del sistema de alguna actividad inusual dentro del sistema que puede ser provocada por un virus de computadora.

No solamente debe protegerse al sistema en contra de usuarios no autorizados y virus de computadoras, también debe cuidarse en contra de cualquier desastre físico como

el fuego; muchos sistemas cuentan con líneas redundantes y sistemas de respaldo; de este modo en caso de incendio o cualquier otro evento desastroso, los puntos críticos del sistema de comunicación de datos continuarán operando utilizando equipo y medio de transmisión alternativos. Muchas corporaciones que utilizan microondas terrestres o satelitales contratan otro tipo de enlace como respaldo, en caso de que el medio de transmisión primario falle.

Sin embargo, no importa que el sistema cuente con muchos tipos de respaldos, se necesita tener un buen plan de recuperación en caso de desastres. La seguridad en cualquier sistema de comunicación de datos se puede mejorar ampliamente teniendo un plan funcional y bien diseñado de recuperación en caso de desastres, el cual es resultado de una buena administración del sistema de comunicación de datos.

e) Requerimientos de Distancia

La distancia entre el emisor y el receptor puede determinar el tipo de medio de transmisión utilizado para el intercambio de información. Además los requerimientos de distancia deben ser medidos en contra del volumen de datos que necesitan transmitirse: si dos sucursales están solamente a unos cuantos metros de distancia, pero el volumen de datos transmitidos es demasiado grande, como cuando se utiliza tecnología multimedia, la fibra óptica puede ser una mejor solución que el par trenzado.

Asimismo, en los medios de transmisión guiados la distancia afecta tanto al número de dispositivos que pueden ser conectados a la red, así como la calidad de la señal debido a que ésta sufre una degradación conforme aumenta la distancia, por lo que se requiere colocar repetidores a cierta distancia (dependiendo del medio de transmisión) para regenerarla.

El costo de los repetidores debe ser tomado en consideración al momento de diseñar el sistema de comunicación de datos; además, para largas distancias los negocios comunes tienen que confiar en los enlaces de los proveedores locales, de microondas terrestres o satelitales.

f) Medio Ambiente

El entorno en el que el medio de transmisión debe existir eliminará algunas opciones para su implantación en el sistema de comunicación de datos. Por ejemplo, en el caso donde las líneas telefónicas comparten la tubería con cables eléctricos, se provocará demasiada interferencia con la transmisión digital de datos.

Durante la etapa de planeación de la red de comunicación de datos, la ubicación del medio y las restricciones locales deben ser tomadas en cuenta para evitar modificaciones costosas durante la instalación.

Por lo tanto se debe tener mucho cuidado de asegurar que la estrategia de comunicación adoptada sea compatible con el medio de transmisión disponible.

g) Mantenimiento

El tipo de mantenimiento requerido para una red de comunicaciones también debe ser considerado durante el proceso de planeación: si el medio de transmisión sufre algún daño, el punto de falla debe ser detectado rápidamente y no debe afectar a toda la estructura de la red. Sin embargo, en el caso de que la falla se presente en un satélite y sea necesario hacer alguna reparación, el tiempo requerido para realizar esta operación puede ser demasiado grande, por lo que es conveniente tener un enlace redundante.

Asimismo, el número de personas requeridas para el mantenimiento de un sistema de comunicaciones de datos basado en microondas no es el mismo que para una red local basada en cables de par trenzado. Aún cuando una estrategia de comunicación de datos puede parecer la mejor solución en términos de su disponibilidad, el mantenimiento y el costo del personal requerido para desarrollar dicho mantenimiento, puede hacer al sistema más costoso que efectivo.

Estas comparaciones económicas deben ser realizadas durante la etapa de planeación del sistema y deben utilizarse para encontrar una solución que no solamente resuelva las necesidades de comunicación de la compañía, sino también que sea factible.

6.3. Consideraciones para el Diseño de la Red Empresarial (LAN / WAN)

6.3.1. Descripción General

Uno de los pasos más importantes para garantizar el desarrollo de una red rápida y estable es su diseño. Si una red no está diseñada de forma adecuada, pueden surgir muchos problemas imprevistos y se puede poner en peligro su crecimiento. El proceso de diseño es verdaderamente un proceso exhaustivo.

Asimismo los administradores de redes de hoy deben administrar redes complejas como las WAN para soportar el número creciente de aplicaciones de software que se desarrollan en torno al protocolo IP y la WWW. Estas WAN exigen una gran cantidad de recursos de la red, y necesitan tecnologías de red de alto desempeño. "Las WAN son entornos complejos que incorporan múltiples medios, múltiples protocolos, e interconexión con otras redes, como Internet"[4]. El crecimiento y la facilidad de administración de estos entornos de red se logra mediante la compleja interacción de protocolos y funciones.

A pesar de las mejoras en el desempeño de los equipos y las capacidades de los medios, el diseño de una red empresarial es una tarea cada vez más difícil; el diseño cuidadoso de ellas puede reducir los problemas asociados con los entornos crecientes de red. Para desarrollar un diseño que sea confiable y escalable, los diseñadores de red deben tener en mente que cada red posee requisitos de diseño específicos.

[4] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Segundo Año".

6.3.2. Objetivos del Diseño

Una red requiere muchas funciones para ser escalable y fácil de administrar. Para diseñar redes confiables y escalables, los diseñadores de red deben darse cuenta de que cada uno de los componentes principales de una red tiene requisitos de diseño específicos.

El primer paso en el proceso de diseño es comprender los requisitos de la empresa, los cuales deben reflejar los objetivos, características, procesos empresariales y políticas de la institución en la que opera. Además se deben establecer y documentar los objetivos de diseño; estos objetivos son específicos para cada organización o situación. Sin embargo, los siguientes requisitos tienden a aparecer en la mayoría de los diseños de red:

- *Funcionalidad.* La red debe ser útil. Es decir, debe permitir que los usuarios cumplan con sus requisitos laborales. La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.
- *Escalabilidad.* La red debe poder aumentar de tamaño. Es decir, el diseño original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.
- *Adaptabilidad.* La red debe estar diseñada teniendo en cuenta las tecnologías futuras y no debe incluir ningún elemento que limite la implantación de nuevas tecnologías a medida que se tornan disponibles.
- *Facilidad de administración.* La red debe estar diseñada para facilitar su monitoreo y administración para asegurar una estabilidad de funcionamiento constante.

Estos requisitos son específicos para ciertos tipos de redes y más generales en otros tipos.

El diseño de una WAN puede ser una tarea sumamente difícil. Se deben analizar varias áreas cuidadosamente al planificar su implantación. Las empresas pueden mejorar constantemente sus WAN incorporando estos pasos al proceso de planeación.

El diseño e implantación de las WAN tiene dos objetivos primarios:

- *Disponibilidad de aplicaciones.* Las redes transportan información de aplicaciones entre computadoras. Si las aplicaciones no están disponibles para los usuarios de la red, la red no está cumpliendo su función.
- *Costo total de propiedad.* El presupuesto de los departamentos de Sistemas de Información a menudo alcanzan los millones de dólares. A medida que las empresas aumentan el uso de los datos electrónicos para administrar las actividades empresariales los costos asociados con los recursos informáticos seguirán creciendo. Una WAN bien diseñada puede ayudar a equilibrar estos objetivos. Cuando se implanta correctamente, la infraestructura de la WAN puede optimizar la disponibilidad de las aplicaciones y permitir el uso económico de los recursos de red existentes.

En general, las necesidades de diseño de la WAN deben tener en cuenta tres factores generales:

- *Variables de entorno.* Las variables de entorno incluyen la ubicación de hosts, servidores, terminales y otros nodos finales, el tráfico proyectado para en el entorno y los costos proyectados de la entrega de diferentes niveles de servicio.
- *Límites de desempeño.* Los límites de desempeño consisten en la confiabilidad de la red, el rendimiento de tráfico, y las velocidades de computación host/cliente (por ejemplo, tarjetas de red y velocidades de acceso del disco duro).
- *Variables de red.* Las variables de red incluyen la topología de la red, capacidades de línea y tráfico de paquetes.

"El objetivo general del diseño es minimizar el costo basándose en estos elementos, proporcionando servicios que no comprometan los requisitos de disponibilidad establecidos. Hay dos aspectos fundamentales: disponibilidad y costo. Estos aspectos se encuentran esencialmente en posiciones antagónicas. Cualquier aumento en la disponibilidad en general debe reflejarse en un aumento en los costos. Por lo tanto, se debe analizar cuidadosamente la importancia relativa de la disponibilidad de recursos y el costo general"[5].

6.3.3. Factores que Afectan el Diseño de una Red

Para diseñar una red con tecnologías de alta velocidad y aplicaciones basadas en multimedia, los diseñadores de red deben hacer frente a los siguientes componentes críticos de diseño general:

a) Función y ubicación de los servidores.
b) Detección de colisiones (para el caso de la tecnologías de Bus) y segmentación.
c) Dominios de ancho de banda versus dominios de broadcast.

a) Función y Ubicación de los Servidores

Una de las claves para diseñar una red exitosa es comprender la función y la ubicación de los servidores que son necesarios para la red. Los servidores suministran archivos compartidos, impresión, comunicación y servicios de aplicación, tales como procesamiento de texto. Los servidores normalmente no funcionan como estaciones de trabajo; en cambio, ejecutan sistemas operativos especializados, tales como NetWare, Windows NT, UNIX y Linux. En la actualidad, cada servidor por lo general está dedicado a una función, por ejemplo, correo electrónico o archivos compartidos.

"Los servidores se pueden clasificar en dos clases distintas: servidores empresariales y servidores de grupo de trabajo. Un servidor empresarial soporta todos los usuarios en la red ofreciendo servicios, tales como correo electrónico o DNS (Domain

[5] Ídem.

Name System). Por otra parte, el servidor de grupo de trabajo soporta un conjunto de usuarios específico brindando servicios tales como procesamiento de texto y archivos compartidos, que son servicios que sólo unos pocos grupos de personas necesitan"[6].

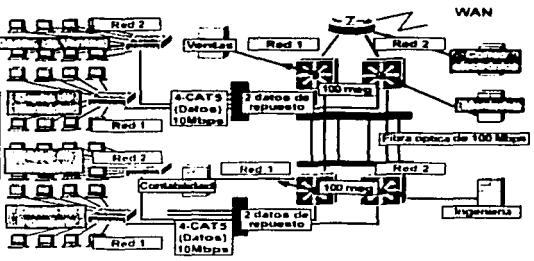


Figura 6.1: Ubicación de los servidores empresariales.

Los servidores empresariales se deben colocar en el cuarto principal de telecomunicaciones; de esta forma, el tráfico hacia los servidores empresariales sólo tiene que viajar hacia este punto y no es necesario que se transmita a través de otras redes. Lo ideal es que los servidores de grupo de trabajo se coloquen en el cuarto intermedio de telecomunicaciones más cercano a los usuarios que accesan a las aplicaciones en estos servidores (Figura 6.1). Al colocar servidores de grupo de trabajo cerca de los usuarios, el tráfico sólo debe viajar a través de la infraestructura de la red hasta el cuarto intermedio de telecomunicaciones y no afecta a los demás usuarios en ese segmento de red.

La ubicación de los servidores en relación con quienes accesan a ellos afecta los patrones de tráfico en la WAN. Si se coloca un servidor empresarial en la capa de acceso del Sitio 1 todo el tráfico destinado a ese sitio se ve forzado a pasar por los enlaces entre los Routers 1 y 2. Esto consume cantidades importantes de ancho de banda desde el Sitio 1 (Figura 6.2).

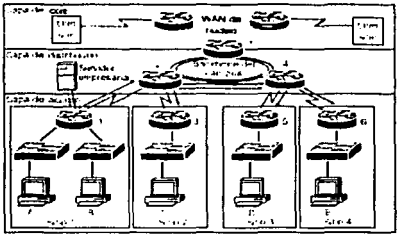


Figura 6.2: Ubicación de los servidores.

El tráfico innecesario consume ancho de banda.

Si se coloca el servidor empresarial en una capa superior de la jerarquía, el tráfico en el enlace entre los Routers 1 y 2 se reduce y queda disponible para que los usuarios en el Sitio 1 accesen a otros servicios (Figura 6.3).

[6] Idem.

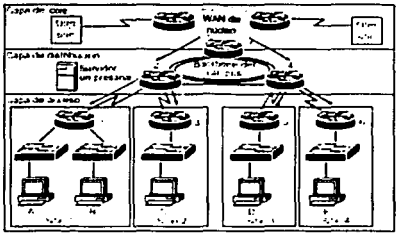


Figura 6.3: Reubicación de los servidores.

El desplazamiento de servidores a ubicaciones correctas libera ancho de banda en la WAN.

En la figura 6.4 se coloca un servidor de grupo de trabajo en la capa de acceso del sitio donde se ubica la mayor concentración de usuarios y el tráfico que atraviesa el enlace WAN para accesar a este servidor es limitado. De esta manera, hay más ancho de banda disponible para accesar a los recursos desde fuera del sitio.

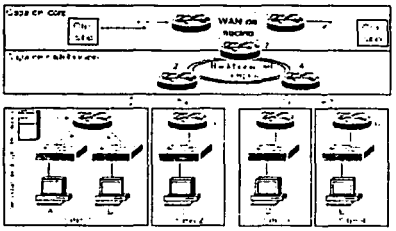


Figura 6.4: Ubicación de los servidores en base a políticas.

-Ubicación de servidores según los usuarios.
- Servidores empresariales vs. servidores de grupo de trabajo.

b) Dominios de Broadcast y Segmentación

Segmentación es el proceso por el cual un solo dominio de colisión se divide en dos o más dominios de colisión (Figura 6.5). Los puentes o switches de Capa 2 (capa de enlace de datos) se pueden utilizar para segmentar una topología de bus lógica y crear dominios de colisión separados, lo que da como resultado que haya una mayor cantidad de ancho de banda disponible para las estaciones individuales.

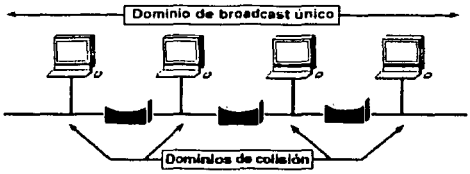


Figura 6.5: Segmentación en una topología de bus.

- Múltiples dominios de colisión.
- Solo hay un dominio de Broadcast.
- Existe un ancho de banda dedicado.

c) Dominios de Ancho de Banda y Dominios de Broadcast

Dominio de ancho de banda es todo lo que está relacionado con un puerto en un puente o switch. En el caso de un Switch Ethernet, el dominio de ancho de banda también se denomina dominio de colisión. Todas las estaciones de trabajo dentro de un dominio de ancho de banda compiten por el mismo recurso de ancho de banda en la red. Todo el tráfico desde cualquier host en el dominio de ancho de banda es visible para todos los demás hosts. En el caso de un dominio de colisión Ethernet, dos estaciones pueden transmitir al mismo tiempo, provocando una colisión (Figura 6.6).

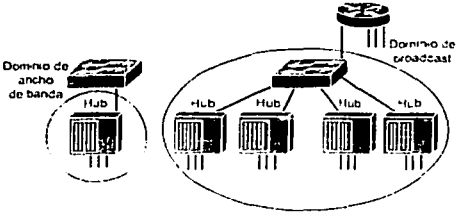


Figura 6.6: Dominio de ancho de banda vs. Dominio de broadcast.

6.3.4. Requisitos de Diseño WAN

La comunicación WAN se produce entre áreas geográficamente separadas. Cuando una estación final local desea comunicarse con una estación remota (es decir, una estación final ubicada en un sitio diferente), la información se debe enviar a través de uno o más enlaces WAN. Los routers dentro de las WAN son puntos de conexión en una red; estos routers determinan la ruta más adecuada a través de la red para las corrientes de datos requeridas.

Las tecnologías de conmutación por circuito y por paquete son dos tipos de servicios WAN, cada uno de los cuales presenta ventajas y desventajas. Por ejemplo, "las redes conmutadas por circuito ofrecen a los usuarios ancho de banda dedicado al que otros usuarios no pueden accesar. Por otro lado, la conmutación por paquetes es un método en el que los dispositivos de red comparten un solo enlace punto a punto para transportar paquetes desde un origen hasta un destino a través de una red portadora"[7]. Las redes conmutadas por paquete tradicionalmente han ofrecido mayor flexibilidad y uso más eficiente del ancho de banda de red que las redes conmutadas por circuito.

Tradicionalmente, las características de la comunicación WAN han sido rendimiento relativamente bajo, alto retardo y elevados índices de error. Las conexiones WAN también se caracterizan por el costo del alquiler de los medios (es decir, los cables) a un proveedor de servicios para conectar dos o más sucursales entre sí. Como la infraestructura WAN a menudo se arrienda a un proveedor de servicio, el diseño WAN debe optimizar el costo y eficiencia del ancho de banda. Por ejemplo, todas las tecnologías

[7] Ford, Merilee. 1998. Ed. Prentice-Hall. "Tecnologías de Interconectividad de Redes".

y funciones utilizadas en las WAN son desarrolladas para cumplir con los siguientes requisitos de diseño:

- Optimizar el ancho de banda de la WAN.
- Minimizar el costo.
- Maximizar el servicio efectivo a los usuarios finales.

Recientemente, las redes tradicionales de medios compartidos se están viendo sobrecargadas debido a los siguientes nuevos requisitos de las redes:

- El uso de las redes ha aumentado a medida que aumenta el uso por parte de las empresas de aplicaciones cliente/servidor, multimedia, y otras aplicaciones para aumentar la productividad.
- La velocidad de los cambios en los requisitos de las aplicaciones se ha acelerado y lo seguirá haciendo (por ejemplo, las tecnologías impulsadas por Internet).
- Cada vez más, las aplicaciones requieren calidades de servicio de red diferenciadas debido a los servicios que proporcionan a los usuarios finales.
- Una cantidad sin precedentes de conexiones se están estableciendo entre oficinas de todos los tamaños, usuarios remotos, usuarios móviles, sitios internacionales, clientes/proveedores e Internet.
- Este crecimiento explosivo de las redes internas y externas corporativas ha creado una mayor demanda de ancho de banda.
- El mayor uso de los servidores empresariales continúa creciendo para satisfacer las necesidades de las organizaciones.

En comparación con las WAN actuales, las nuevas infraestructuras WAN deben ser más complejas, basándose en nuevas tecnologías, y deben poder manejar combinaciones de aplicaciones cada vez con niveles de servicio requeridos y garantizados. Además, con un aumento estimado del 300% en la cantidad de tráfico para los próximos cinco años, las empresas sufrirán una presión aún mayor para limitar los costos de las WAN.

Los diseñadores de redes están usando las tecnologías WAN para soportar estos nuevos requisitos. Las conexiones WAN generalmente manejan información importante y están optimizadas en el aspecto del precio y desempeño del ancho de banda. Los routers que conectan sucursales, por ejemplo, generalmente aplican optimización del tráfico, múltiples rutas para redundancia, respaldo de información para la recuperación de desastres y calidad de servicio para las aplicaciones críticas.

6.3.5. Metodología del Diseño de la Red Empresarial

Para que una red sea efectiva y sirva para las necesidades de los usuarios, debe diseñarse e implantarse de acuerdo con una serie de pasos sistemáticos planificados, que incluyen lo siguiente:

- Reunión de los requisitos y las expectativas de los usuarios.
- Análisis de los requisitos.

- Diseño de la estructura (es decir, la topología) de Capas 1, 2 y 3 del modelo OSI.
- Documentación de la implantación física y lógica.

a) Reunión de Requisitos

El primer paso para diseñar una red debe ser reunir datos acerca de la estructura y los procesos de la organización. Esta información incluye el historial de la organización y su estado actual, el crecimiento proyectado, las políticas operativas y los procedimientos de administración, los sistemas y procedimientos de oficina y los puntos de vista de las personas que utilizarán la red (Figura 6.7).

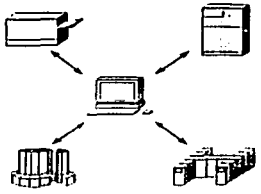


Figura 6.7: Reunión de requisitos.

- **Estructura corporativa.**
- **Flujo de información comercial.**
- **Aplicaciones en uso.**
- **Topología actual (si existe).**
- **Características de desempeño de la red actual (si existe).**

A continuación es necesario determinar cuáles son las personas más importantes que pueden ayudar a diseñar la red. Es necesario hablar con los principales usuarios y averiguar su ubicación geográfica, sus aplicaciones actuales y sus necesidades proyectadas. "Se necesitan contestar las siguientes preguntas: ¿Quiénes son las personas que utilizarán la red? ¿Cuál es su nivel de capacidad y cuáles son sus actitudes acerca de las computadoras y de las aplicaciones informáticas?. Si se responden estas preguntas y otras similares, esto ayudará a determinar cuanta capacitación será necesaria y cuantas personas se necesitan para soportar la red. El diseño final de red debe reflejar los requisitos de los usuarios.

Lo ideal es que el proceso de reunión de información ayude a clarificar e identificar los problemas. También se debe determinar si hay políticas documentadas en vigencia. ¿Algunos de los datos han sido declarados críticos para el trabajo? ¿Algunas operaciones han sido declaradas críticas para el trabajo? (Los datos y las operaciones críticos para el trabajo son aquellos que se consideran fundamentales para la empresa, y el acceso a ellos es crucial para las actividades que se ejecutan diariamente). ¿Cuáles son los protocolos que están permitidos en la red? ¿Sólo se soportan determinados hosts de escritorio?"[8].

Posteriormente, se debe determinar cuál es la persona dentro de la organización que tiene autoridad sobre el direccionamiento, la denominación, el diseño de topología y la configuración. Algunas empresas cuentan con un departamento central de Sistemas de Información de Administración, MIS (Management Information System) que controla todo. Algunas empresas cuentan con varios departamentos MIS pequeños y, por lo tanto, deben delegar la autoridad a los mismos.

[8] Cisco Systems, Inc. 2002. Ed. Pearson Educación. "Academia de Networking de Cisco Systems: Guía del Segundo Año".

El enfoque se debe centrar en la identificación de recursos y limitaciones de la organización. "Los recursos de la organización que pueden afectar la implantación de un nuevo sistema de red se clasifican en dos categorías generales: hardware/software informático y recursos humanos. El hardware y el software informático existente de una organización se debe documentar y se deben identificar las necesidades de hardware y software proyectadas. ¿Cómo se vinculan y comparten estos recursos actualmente? ¿Cuáles son los recursos financieros de los que dispone la organización?"[9]. La documentación de esta clase de cosas ayudará a estimar los costos y desarrollar un presupuesto para la red. Se debe asegurar que se comprenden las cuestiones relacionadas con el desempeño de cualquier red existente.

En general, los usuarios primordialmente necesitan disponibilidad de las aplicaciones en sus redes. Los componentes principales de la disponibilidad de las aplicaciones son el tiempo de respuesta, rendimiento y confiabilidad:

- El tiempo de respuesta es el tiempo que transcurre entre la introducción de un comando o presión de una tecla y la ejecución por parte del sistema del comando o la entrega de una respuesta. Las aplicaciones en las que el tiempo rápido de respuesta se considera crítico incluyen los servicios interactivos en línea como los cajeros automáticos y las máquinas de punto de venta.
- Las aplicaciones que necesitan rendimiento generalmente involucran actividades de transferencia de archivos. Sin embargo, las aplicaciones que necesitan gran cantidad de rendimiento normalmente tienen requisitos bajos de tiempo de respuesta. De hecho, a menudo se pueden programar en los momentos en los que el tráfico sensible a los tiempos de respuesta es bajo (por ejemplo, después de las horas normales de trabajo).
- Aunque la confiabilidad siempre es importante, algunas aplicaciones tienen requisitos genuinos que superan las necesidades típicas. Las organizaciones que llevan a cabo todas sus actividades en línea o por teléfono requieren casi 100% de tiempo de actividad. Los servicios financieros, bolsas de valores y las operaciones de emergencias, policía y militares son algunos ejemplos. Estas situaciones requieren un alto nivel de hardware y redundancia. La determinación del costo del tiempo de inactividad es fundamental para determinar la importancia de la confiabilidad de la red.

Hay varias maneras de analizar los requisitos de los usuarios. Cuanto más involucrados estén los usuarios en el proceso, más probabilidades hay de que la evaluación sea precisa. En general, se pueden usar los siguientes métodos para obtener esta información:

- Perfiles de comunidad de usuarios. Esquema de lo que necesitan los diferentes grupos de usuarios. Este es el primer paso en la determinación de los requisitos de red. Aunque la mayoría de los usuarios generales tienen los mismos

[9] Idem.

requisitos de correo electrónico, también pueden necesitar otras cosas, como compartir los servidores de impresión en sus áreas.

- Se puede obtener información de base para la implantación de una red mediante entrevistas, grupos de enfoque y encuestas. Se debe comprender que algunos grupos pueden requerir acceso a servidores comunes. Otros pueden necesitar que se les permita acceso externo a recursos informáticos internos específicos. Ciertas organizaciones pueden requerir sistemas de soporte de sistemas de información que se puedan administrar de una manera específica, según algún estándar externo.
- El método menos formal de obtener información es realizar entrevistas con grupos de usuarios clave. Los grupos de enfoque también se pueden usar para reunir información y generar discusiones entre diferentes organizaciones que tengan intereses similares (o distintos). Finalmente, se pueden usar encuestas formales para obtener una lectura estadísticamente válida de las opiniones de los usuarios con respecto a un nivel de servicio en particular.
- Pruebas de factores humanos. El método más caro, más tardado y posiblemente más revelador de evaluación de los requisitos de los usuarios es realizar una prueba que involucre a los usuarios representativos en un entorno de laboratorio. Esto se puede aplicar mejor cuando se evalúan los requisitos de tiempo de respuesta. Por ejemplo, se pueden configurar sistemas de trabajo y hacer que los usuarios ejecuten actividades de host remoto normales desde la red de laboratorio. Mediante la evaluación de las reacciones de los usuarios ante las variaciones en la capacidad de respuesta del host, se pueden crear umbrales de referencia para el desempeño aceptable.

Después de reunir datos acerca de la estructura corporativa, es necesario determinar dónde fluye la información en la empresa. Averiguar dónde residen los datos compartidos y quiénes los usan. Determinar si se puede accesar a los datos que se encuentran fuera de la empresa. Se debe asegurar que se comprenden los aspectos relacionados con el desempeño de cualquier red existente. Si el tiempo lo permite, analizar el desempeño de la red actual.

b) Análisis de Requisitos

"Es necesario analizar los requisitos de red, incluyendo los objetivos técnicos y empresariales del cliente. ¿Cuáles son las aplicaciones que se implantarán? ¿Hay aplicaciones que utilizan Internet? ¿Cuáles son las redes a las que se accesará? ¿Cuáles son los criterios de éxito?"[10] (Figura 6.8).

La disponibilidad mide la utilidad de la red. Muchas cosas afectan la disponibilidad, incluyendo el rendimiento, el tiempo de respuesta y el acceso a los recursos. Cada cliente tiene una definición distinta de lo que es la disponibilidad. Se puede incrementar la disponibilidad agregando más recursos, lo cual provoca el aumento del costo. El diseño de red trata de suministrar la mayor disponibilidad posible al menor costo posible.

[10] Idem.

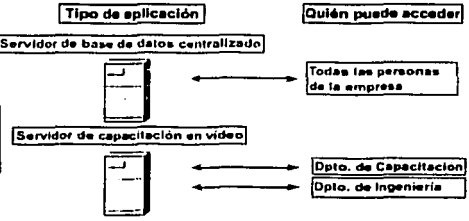


Figura 6.8: Análisis de requisitos.

El objetivo del análisis de los requisitos es determinar las velocidades promedio y pico para cada origen en el tiempo. Se debe intentar caracterizar la actividad durante un día normal de trabajo en términos del tipo de tráfico, nivel de tráfico que se mueve, el tiempo de respuesta de los hosts y el tiempo para ejecutar las transferencias de archivos. También se puede observar la utilización en el equipo de red existente durante el período de prueba.

Si las características probadas de la red se aproximan a las de la nueva red, se pueden estimar los requisitos de la nueva red según la cantidad proyectada de usuarios, aplicaciones y topología. Ésta siempre será una estimación aproximada del tráfico, dada la falta de herramientas que sirvan para medir el comportamiento detallado del mismo.

Además de monitorear pasivamente una red existente, se puede medir la actividad y el tráfico generado por una cantidad conocida de usuarios conectados a una red de prueba representativa y luego calcular lo que se haya descubierto sobre la población anticipada.

"Uno de los problemas de la definición de las cargas de trabajo en las redes es que es difícil descubrir con precisión la carga de tráfico y el desempeño de los dispositivos de red en función de la cantidad de usuarios, tipo de aplicación y ubicación geográfica; esto es particularmente verdadero cuando no existe instalada una red"[11].

Se deben tener en cuenta los siguientes factores que influirán en la dinámica de la red:

- La naturaleza dependiente del tiempo de las horas pico de acceso a la red pueden variar. Las mediciones deben reflejar una gama de observaciones que incluyen la demanda en estos períodos.
- Las diferencias asociadas con el tipo de tráfico (tráfico ruteado y switcheado) plantean diferentes exigencias sobre los dispositivos y protocolos de la red. Algunos protocolos pueden detectar los paquetes descartados. Algunos tipos de aplicación exigen mayor cantidad de ancho de banda.
- La naturaleza aleatoria del tráfico de red. El tiempo exacto de llegada y los efectos específicos del tráfico son impredecibles.

[11] Idem.

Cada fuente de tráfico tiene su propia métrica, y cada una se debe convertir a bits por segundo. Se deben estandarizar los volúmenes de tráfico para obtener volúmenes por usuario. Por último, se debe aplicar un factor que tenga en cuenta los gastos de protocolo, fragmentación de paquetes, crecimiento de tráfico y margen de seguridad. Con la variación de este factor se pueden realizar análisis de probabilidades (¿qué pasaría si ...?). Por ejemplo, se puede ejecutar Microsoft Office desde un servidor y entonces analizar el volumen de tráfico generado por los usuarios que comparten la aplicación en la red. Este volumen ayuda a determinar el ancho de banda y requisitos del servidor para instalar Microsoft Office en la red.

Otro de los componentes de la fase de análisis es la evaluación de los requisitos del usuario. Una red que no puede suministrar información veloz y precisa a los usuarios no es de mucha utilidad. Por lo tanto, se deben tomar medidas para asegurar que se cumplen los requisitos de información de la organización y sus trabajadores.

c) Diseño de la Estructura de la Red

Una vez que se han determinado los requisitos generales para la red, el siguiente paso es decidir cuál será la topología de red general que satisface los requisitos del usuario.

Las partes principales del diseño de una topología de red se pueden dividir en tres categorías exclusivas del modelo de referencia OSI: la capa de red, la capa de enlace de datos y la capa física (Figura 6.9).

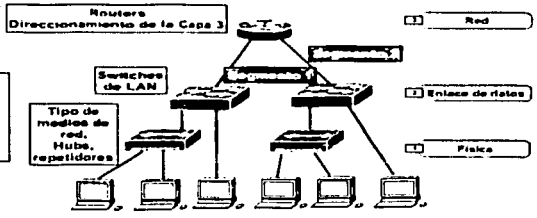


Figura 6.9: Determinación de la topología física a implantar.

d) Documentación de la Topología Física

El diagrama lógico es el modelo de topología de red sin todos los detalles de la ruta de instalación exacta del medio seleccionado; es el mapa de ruta básico de la red. Por ejemplo, Suponiendo que se está utilizando un medio de transmisión guiado, los elementos del diagrama lógico incluirán:

- Las ubicaciones exactas de los centros de cableado (Cuarto de Telecomunicaciones Principal e Intermedios).
- El tipo y la cantidad de cableado que se utiliza para interconectar los Cuartos de Telecomunicaciones Intermedios con el Cuarto Principal de

Telecomunicaciones, así como también la cantidad de cables de repuesto que hay disponibles para aumentar el ancho de banda entre los cuartos para el cableado.

- Documentación detallada sobre todos los tendidos de cable, como se indican en tabla 6.1, el tipo de conexión, los números de identificación del cable y del puerto donde termina el tendido de cableado, el tipo de cable y su estado.

Tabla 6.1: Relación del tendido del cable.

Conexión	ID del Cable	# Puerto	Tipo de Cable	Estado
CTI1 - CTP	CTI 1-1	1	Fibra Multimodo	Utilizado
CTI1 - CTP	CTI 1-2	2	Fibra Monomodo	Libre

6.3.6. Aspectos de la Integración LAN / WAN

Las aplicaciones distribuidas necesitan cada vez más ancho de banda y la explosión en el uso de Internet hace que muchas arquitecturas LAN se utilicen hasta el límite. Las comunicaciones de voz han aumentado significativamente con mayor uso de los sistemas centralizados de correo de voz para las comunicaciones verbales. La red es la herramienta crítica para el flujo de información, por lo que es necesario que las redes cuesten menos, pero que al mismo tiempo soporten las aplicaciones emergentes y la mayor cantidad de usuarios con aumento en el desempeño.

Hasta ahora, las comunicaciones de área local y amplia habían permanecido lógicamente separadas. "En la LAN, el ancho de banda es gratuito y la conectividad se encuentra limitada únicamente por los costos de hardware e implantación. En la WAN, el ancho de banda es el costo más importante y el tráfico sensible a los retardos, como el tráfico de voz, ha permanecido separado del tráfico de datos.

Las aplicaciones de Internet como voz y video en tiempo real requieren un rendimiento de LAN y WAN mejor y más predecible. Estas aplicaciones multimedia rápidamente se están transformando en herramientas fundamentales de productividad empresarial. A medida que las empresas empiezan a tener en cuenta la implantación de nuevas aplicaciones multimedia basadas en redes internas que exigen una gran cantidad de ancho de banda, como capacitación en video, videoconferencias y voz a través de IP"[12]. El impacto de estas aplicaciones sobre la infraestructura existente de red se transformará en un problema serio.

Por ejemplo, si una empresa utiliza su red corporativa para el tráfico IP fundamental para la empresa y desea integrar una aplicación de capacitación por video, la red debe poder proporcionar calidad de servicio garantizada; esta calidad de servicio debe entregar el tráfico multimedia, pero no debe permitir que interfiera con el tráfico crítico para la empresa. Como consecuencia, los diseñadores de la red necesitan mayor flexibilidad para resolver múltiples problemas de red sin crear múltiples redes o basarse en las inversiones de comunicación de datos existentes.

[12] Idem.

a) Prueba de Sensibilidad de la Red Empresarial

Desde el punto de vista práctico, la prueba de sensibilidad involucra la interrupción de enlaces estables y observar lo que sucede. Cuando se trabaja con una red de prueba, esto es relativamente fácil. Se pueden provocar perturbaciones en la red eliminando una interfaz activa, y monitorear cómo el cambio es manejado por la red: cómo se redirecciona el tráfico, la velocidad de convergencia, si se pierde conectividad, y si surgen problemas al manejar tipos específicos de tráfico. También se puede cambiar el nivel de tráfico en una red para determinar sus efectos sobre ella cuando los niveles de tráfico se aproximan a la saturación de los medios.

6.4. Modelos para la Implantación de la Red Empresarial

6.4.1. Uso del Modelo OSI en el Diseño de la Red

Después de comprender los requisitos de red, es necesario identificar y luego diseñar el entorno informático para cumplir con estos requisitos.

Los modelos jerárquicos para el diseño de red permiten diseñar redes en capas. Para comprender la importancia de la división en capas, tomemos como ejemplo el modelo de referencia OSI, un modelo dividido en capas, para comprender las comunicaciones informáticas. "Los modelos jerárquicos para el diseño de red también usan capas para simplificar las tareas requeridas para la red. Cada capa se puede centrar en funciones específicas permitiendo, de este modo, que el diseñador de red elija los sistemas y funciones para esa capa"[13].

El uso de un diseño jerárquico puede facilitar los cambios. La modularidad en el diseño de red permite crear elementos de diseño que se pueden replicar a medida que crece la red. Además, como las redes siempre requieren actualizaciones, el costo y la complejidad de la actualización se limitan a un pequeño subconjunto de toda la red. En las arquitecturas planas o en malla de gran tamaño, los cambios tienden a afectar una gran cantidad de sistemas. Se puede facilitar la identificación de puntos de falla en una red estructurándola en elementos pequeños y de fácil comprensión. Los administradores de red pueden comprender fácilmente los puntos de transición en la red, lo que ayuda a identificar los puntos de falla.

6.4.2. Modelo Jerárquico de Red

"Los diseños de red generalmente siguen una de dos estrategias generales de diseño: de malla o jerárquica. En una estructura de malla, la topología es plana, todos los dispositivos de comunicaciones de datos ejecutan esencialmente las mismas funciones y generalmente, no hay una definición clara del lugar donde se ejecutan las funciones específicas. La expansión de la red tiende a desarrollarse de manera arbitraria y no

[13] Ídem.

planificada. En una estructura jerárquica, la red se organiza en capas, cada una de las cuales cumple una o más funciones específicas"[14].

Las ventajas del uso de un modelo jerárquico incluyen las siguientes:

- *Escalabilidad.* Las redes que siguen el modelo jerárquico pueden aumentar de tamaño sin sacrificar el control o facilidad de administración, ya que la funcionalidad se encuentra limitada a una ubicación en particular y los problemas potenciales se pueden reconocer con mayor facilidad. Un ejemplo de diseño de una red jerárquica muy grande es la red telefónica pública conmutada.
- *Facilidad de implantación.* Un diseño jerárquico asigna funcionalidad clara a cada capa, facilitando por lo tanto su implantación.
- *Facilidad para el diagnóstico de fallas.* Como las funciones de las capas individuales se encuentran bien definidas, el aislamiento de los problemas en la red es menos complicado. También es más fácil segmentar temporalmente la red para reducir el alcance de un problema.
- *Capacidad de predicción.* El comportamiento de una red utilizando capas funcionales es bastante predecible, lo que hace que la planificación de la capacidad para el crecimiento sea mucho más fácil. Este enfoque de diseño también facilita la creación de un modelo de desempeño de una red para fines analíticos.
- *Soporte de protocolo.* La mezcla de aplicaciones y protocolos actuales y futuros es mucho más fácil en las redes que siguen los principios del diseño jerárquico porque la infraestructura subyacente ya se encuentra lógicamente organizada.
- *Facilidad de administración.* Todas las ventajas que se enumeran aquí contribuyen a hacer que la red sea más fácil de administrar.

a) Diseño Jerárquico de Tres Capas

Un diseño de red jerárquico incluye las siguientes tres capas (Figura 6.10):

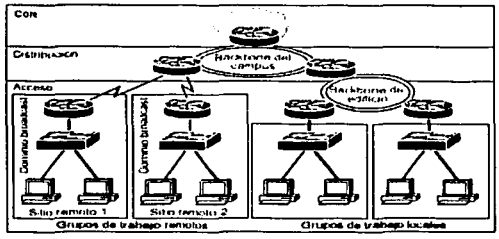


Figura 6.10: Diseño de red jerárquico.

- La capa de core (núcleo). Proporciona transporte óptimo entre sitios.
- La capa de distribución. Brinda conectividad basada en políticas.

[14] Idem.

- La capa de acceso. Proporciona acceso para los usuarios y grupos de trabajo a la red.

1. Descripción de los Componentes del Modelo de Diseño de Tres Capas

"Una capa se identifica como el punto de la red donde se produce un límite de Capa 3 del modelo de referencia OSI (capa de red). Las tres capas se encuentran conectadas por dispositivos de Capa 3 u otros dispositivos que dividen la red en dominios de broadcast, en el caso de redes con topología de bus"[15] (Figura 6.10), el modelo de tres capas se compone de las capas de core, de distribución y de acceso, cada una de las cuales tiene funciones específicas:

- *Capa de core.* Esta capa proporciona conexiones rápidas WAN entre sitios separados por grandes distancias geográficas, uniendo varias redes de campus en una WAN corporativa o empresarial. Los enlaces de core son normalmente punto a punto, y rara vez hay hosts en esta capa. Los servicios de core (por ejemplo, E1/E3, Frame Relay, X.25) normalmente son arrendados a un proveedor de servicios de telecomunicaciones.
- *Capa de distribución.* Esta capa ofrece servicios de red a múltiples LAN dentro de un entorno WAN. Aquí es donde se encuentra la red backbone de la WAN, y normalmente se basa en FastEthernet o GiabitEthernet. Esta capa se implanta en grandes sitios y se usa para interconectar edificios.
- *Capa de acceso.* La capa de acceso normalmente es una LAN o grupo de LAN, normalmente Ethernet o Token Ring, que ofrece a los usuarios acceso frontal a los servicios de red. La capa de acceso es donde casi todos los hosts se conectan a la red, incluyendo servidores de todo tipo y estaciones de trabajo.

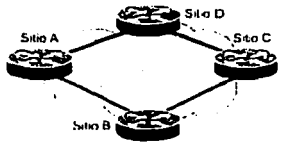
Un modelo de tres capas puede satisfacer las necesidades de la mayoría de las redes empresariales. Sin embargo, no todos los entornos requieren una jerarquía completa de tres capas. En ciertos casos, un diseño de dos capas puede ser adecuado, o inclusive una red plana de una sola capa. Aún en estos casos, sin embargo, se debe planificar o mantener una estructura jerárquica para permitir que estos diseños de red se expandan a tres capas de ser necesario.

1.1. Funciones de la Capa de Core

"La función de la capa de core es proporcionar una ruta rápida entre sitios remotos (Figura 6.11). Esta capa no debe participar en ninguna manipulación de paquetes, como las listas de control de acceso y el filtrado, que haría que la conmutación de paquetes fuera más lenta. La capa de core normalmente se implanta como una WAN"[16]. La WAN necesita rutas redundantes para que la red pueda soportar cortes de circuito individuales y seguir funcionando. La carga compartida y la convergencia rápida de los protocolos de ruteo también son funciones de diseño importantes. El uso eficiente del ancho de banda en el core siempre es un asunto que merece atención.

[15] Ídem.
[16] Ídem.

Figura 6.11: La capa de core.



- **Rutas redundantes.**
- **Compartir la carga.**
- **Rápida convergencia.**
- **Uso eficiente del ancho de banda.**

1.2. Funciones de la Capa de Distribución

"La capa de distribución es el punto de demarcación entre las capas de acceso y de core y ayuda a definir y diferenciar el core. El propósito de esta capa es proporcionar definición de límites y es la capa en la que se produce la manipulación de paquetes"[17]. En un entorno WAN, la capa de distribución puede incluir varias funciones, como las siguientes:

- Unificación de direcciones o áreas.
- Acceso de departamentos o de grupos de trabajo a la capa de core.
- Definición de dominio de Broadcast/Multicast (en el caso de Ethernet).
- Ruteo de Virtual Local Area Network (VLAN).
- Cualquier transición de medio que deba producirse.
- Seguridad.

La capa de distribución debe incluir el backbone del campus con todos los routers que lo conectan (Figura 6.12). Como las políticas normalmente se implantan en este nivel, se puede decir que la capa de distribución proporciona conectividad basada en políticas, lo que significa que los routers se encuentran programados para permitir solamente tráfico aceptable en el backbone del campus. Se debe notar que las buenas prácticas de diseño de red indican que no se deben poner estaciones finales (como los servidores) en el backbone. Al no colocar las estaciones finales en el backbone, éste se libera para funcionar estrictamente como ruta de tránsito entre grupos de trabajo o servidores de todo el campus.

La capa de distribución también puede ser el punto en el que los sitios remotos accessan a la red corporativa. En resumen, la capa de distribución se puede definir como la capa que proporciona conectividad basada en políticas.

Figura 6.12: La capa de distribución.

- **Control de acceso a los servicios.**
- **Definición de métricas de las rutas.**
- **Control de anuncios de ruteo.**

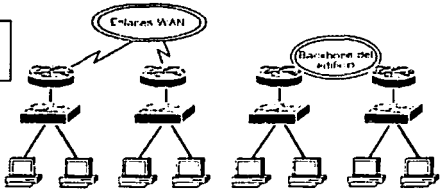
[17] Idem.

1.3. Funciones de la Capa de Acceso

La capa de acceso es el punto en el que los usuarios finales pueden accesar a la red (Figura 6.13). Esta capa también puede usar listas de control de acceso o filtros para optimizar las necesidades de un conjunto de usuarios en particular. Las funciones de la capa de acceso pueden incluir lo siguiente:

- Ancho de banda compartido.
- Ancho de banda conmutado.
- Filtrado de capa MAC.
- Microsegmentación.

Figura 6.13:
La capa de acceso.



- Proporcionar segmentación lógica.
- Usuarios de grupo con intereses comunes.
- Aislar tráfico de broadcast del grupo de trabajo.

La capa de acceso conecta a los usuarios a las LAN, y las LAN a los backbones o enlaces WAN. Este enfoque permite que los diseñadores distribuyan servicios de dispositivos que operan en esta capa. "La capa de acceso permite la segmentación lógica de la red y agrupaciones de usuarios basándose en su función. Tradicionalmente, esta segmentación se basa en los límites de las organizaciones (como los departamentos de mercadotecnia, administración o ingeniería). Sin embargo, desde el punto de vista de administración y control de la red, la función principal de la capa de acceso es aislar el tráfico de broadcast al grupo de trabajo o LAN individual"[18]. La capa de acceso también puede permitir que los sitios remotos accesen a la red corporativa a través de algún tipo de tecnología de área amplia, como Frame Relay.

b) Diseños de Red de Dos Capas

En un diseño de dos capas, se usa un enlace WAN para interconectar sitios separados. "Dentro del sitio se pueden implantar múltiples LAN en las que cada segmento LAN es su propio dominio de broadcast. Por ejemplo el router en el Sitio F se transforma en el punto de concentración de los enlaces WAN (Figura 6.14)"[19].

[18] Ídem.
[19] Ídem.

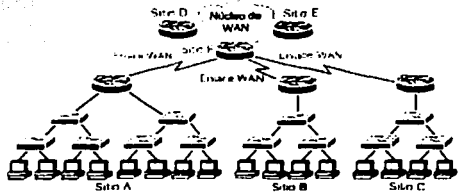


Figura 6.14: Diseño de red de dos capas.

c) Diseños de Red de Una Capa

No todas las redes necesitan una jerarquía de tres capas. "Una decisión de diseño clave es la ubicación de los servidores: se pueden distribuir en múltiples LAN o se pueden concentrar en una ubicación de servidor central. Un diseño de una capa normalmente se implanta si existen unas pocas ubicaciones remotas en la empresa y el acceso a las aplicaciones se realiza principalmente a través de la LAN local al servidor de archivos del sitio. Cada sitio es su propio dominio de broadcast (Figura 6.15)"[20].

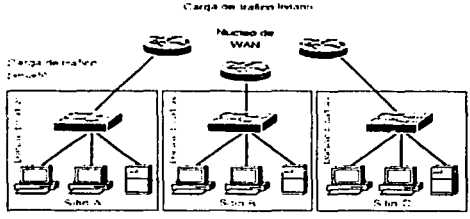


Figura 6.15: Diseño de red de una sola capa.

d) Ventajas de los Diseños Jerárquicos

Una de las ventajas de un diseño jerárquico es que proporciona un método para controlar el tráfico de datos colocando puntos de ruteo de Capa 3 en toda la red. Como los routers tienen la capacidad de determinar rutas desde el host origen a los hosts destino según el direccionamiento de Capa 3, el tráfico de datos fluye hacia arriba en la jerarquía hasta encontrar el host destino (Figura 6.16) .

[20] Idem.

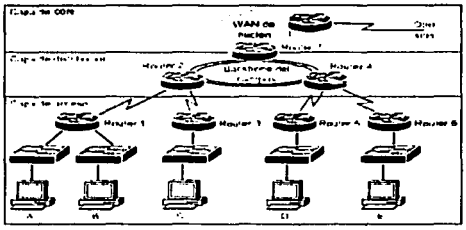


Figura 6.16: Diseño jerárquico de la red.

Si el Host A debe establecer una conexión al Host B, el tráfico desde esta conexión debe ir desde el Router 1 y enviarse de vuelta al Host B. Se puede ver que esta conexión no requiere que haya ningún tráfico en el enlace entre el Router 1 y el Router 2, conservando así el ancho de banda en ese enlace (Figura 6.17).

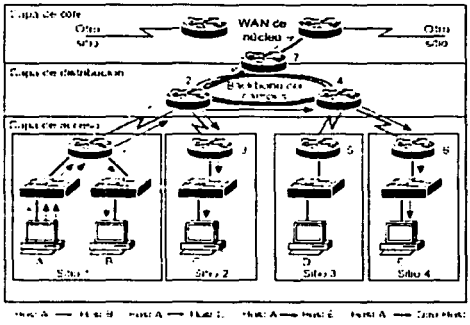


Figura 6.17: Optimización del ancho de banda entre enlaces.

En una jerarquía WAN de dos capas (Figura 6.18), el tráfico sólo recorre la jerarquía hasta el punto en que sea necesario para llegar al destino, conservando de esta manera el ancho de banda en otros enlaces WAN.

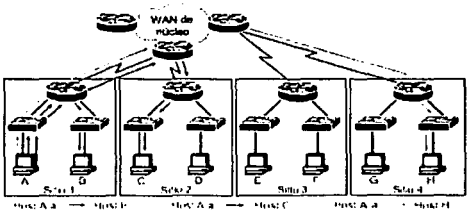


Figura 6.18: Red jerárquica de dos capas.

6.5. Definición de Políticas de Seguridad

6.5.1. Soluciones Generales a las Amenazas Contra la Integridad y Seguridad de los Datos

a) Herramientas para Mejorar la Integridad de los Datos

"Las técnicas preventivas (Figura 6.19) están diseñadas para mantener la integridad de los datos, mientras que las medidas correctivas (Figura 6.20) se utilizan para recuperar la integridad de los datos una vez producida la pérdida"[21].

1. Medidas Preventivas más Comunes

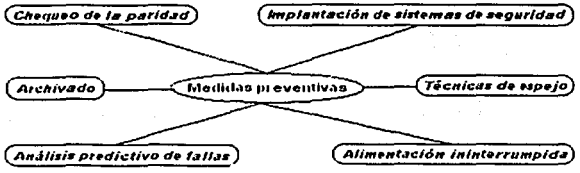


Figura 6.19: Medidas preventivas para la integridad de los datos.

- Técnicas de Espejo. Las técnicas de espejo son aquellas en las que se copian los datos de un dispositivo o máquina a otra diferente según se están escribiendo. Estas técnicas pueden ser realizadas de forma lógica para replicar segmentos del sistema de archivos de una máquina en otra parte de la red.

- Archivado. El archivado se refiere al proceso de borrado de archivos del sistema de almacenamiento online y su copia en elementos de almacenamiento a largo plazo, en cinta o en medios ópticos. Aunque el objetivo principal del archivado puede ser la creación de espacio en volúmenes de almacenamiento mediante el borrado de archivos viejos, también puede ser utilizado para aumentar la protección del sistema de archivos borrando datos del sistema de almacenamiento online y colocándolos en carpetas dispuestas para este fin, protegiéndolos así de las cosas raras que pudieran sucederles.

- Chequeo de Paridad. El chequeo de paridad es una característica de los servidores que suministra un mecanismo de guardia para asegurar que las fallas inesperadas de memoria no tengan como resultado la falla del servidor o la pérdida de la integridad de los datos.

- Análisis Predictivo de Fallas. Es raro que un componente falle completamente de inmediato. Si pudiera observarse un dispositivo que está fallando, podría notarse que comienza comportándose de forma extraña durante algún tiempo, con un número de errores cada vez mayor.

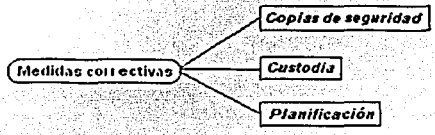
[21] Varios Autores. 1998. Ed. McGraw-Hill. "LAN TIMES. Guía de Seguridad e Integridad de Datos".

- Alimentación Ininterrumpida. El suministro ininterrumpido de energía es uno de los elementos esenciales para las máquinas principales, que se encarga de suministrar las baterías de reserva en caso de pérdida de energía. También brindan un voltaje consistente y sin fluctuaciones a la máquina, lo cual es de gran valor, ya que la red que suministra la energía varía con los cambios de carga, pudiendo afectar a la operación del sistema.

- Implantación de Sistemas de Seguridad. Alejar del sistema a los empleados disgustados, los timadores y los competidores, ayudará a mantener la integridad de los datos.

2. *Medidas Correctivas más Comunes*

Figura 6.20: Medidas correctivas para la integridad de los datos.



- Copias de Seguridad. La realización de copias de seguridad es el método más utilizado para restablecer un sistema en peligro: si se pierde la integridad de los datos, se puede recuperar una copia anterior del sistema a partir de las copias de seguridad.

- Custodia. La custodia hace referencia a la forma en la que se consigue que los respaldos se encuentren en lugares seguros.

- Planificación de Recuperación Frente a Desastres. Un plan de recuperación contra desastres es como una guía que permite la recuperación del sistema desde cero.

b) Herramientas para Reducir las Amenazas Contra la Seguridad

Para reducir las amenazas en contra de la seguridad se pueden implantar las siguientes recomendaciones a través del sistema (Figura 6.21) o a través de las políticas de seguridad de la organización (figura 6.22).

1. *Recomendaciones Implantadas por el Sistema*

- Eliminación de las Puertas Traseras del Sistema. Si se descubre una puerta trasera en el sistema se debería cerrar. Obviamente, esto podría ser un problema si se necesita resolver un error que requiere dicha puerta trasera para accesar al sistema.

- Chequeo de Virus. El chequeo de virus es otro aspecto de vital importancia: hay muchos productos antivirus en el mercado que pueden ayudar a prevenir la invasión de los virus.

- Cifrado. El cifrado descompone los datos de manera que no pueden ser utilizados, a no ser que sean primeramente descifrados. El punto débil de todos los esquemas de cifrado es la utilización de algoritmos que pueden ser finalmente decodificados por otra persona.

- Obligación de Identificación. La identificación que segura la validez de la persona autorizada para accesar al sistema y ejecutar algún programa es extremadamente importante para evitar que personas no autorizadas ejecuten algún tipo de código malicioso.

- Firewalls para el Acceso a Internet. Con el fin de obtener un punto más de seguridad en contra de los ataques provenientes de Internet se recomienda la instalación de un firewall que limite los servicios que pueden ser utilizados en la organización.

- Trampas para Intrusos. Se pueden instalar productos que determinen la identidad de los usuarios y desde donde están trabajando. La idea es hacer creer a los intrusos que se encuentran dentro del sistema, mientras que de forma simultánea, se intenta localizar el nodo del cual procede la intrusión.

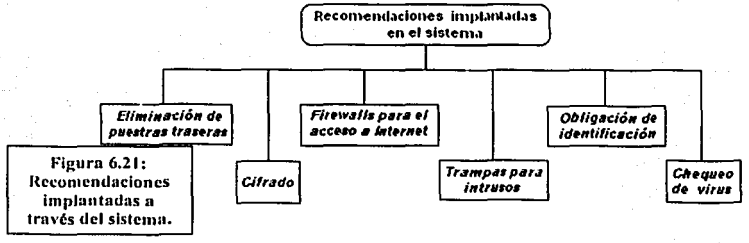


Figura 6.21: Recomendaciones implantadas a través del sistema.

2. *Recomendaciones Implantadas a Través de Políticas*

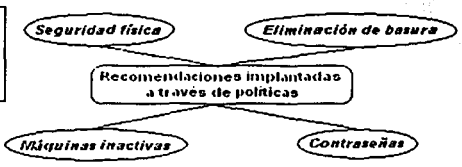
- Seguridad Física. Los equipos que se encuentran en lugares cerrados con llave a los que la mayoría de la gente no tiene acceso son más seguros desde el punto de vista de las amenazas contra la seguridad, que los equipos que se encuentran a la vista donde cualquiera tiene acceso.

- Política de Máquinas Inactivas. Se refiere a la utilización de los protectores de pantalla y las contraseñas de teclado cuando una máquina ha permanecido inactiva por un tiempo determinado.

- Política de Eliminación de Basura. Eliminación periódica de archivos temporales y/o inútiles con el fin de aprovechar adecuadamente los recursos del sistema.

- Política de Contraseñas. Las contraseñas de los usuarios deben cambiarse de forma periódica con el fin de prevenir accesos al sistema de forma ilegal por alguien con una contraseña robada.

Figura 6.22: Recomendaciones implantadas a través de políticas.



6.6. Modelo de Comunicación Seguro

6.6.1. Ingeniería de Seguridad del Sistema

a) Especificación de la Arquitectura del Sistema

Como primer paso en el proceso de ingeniería de seguridad del sistema, la arquitectura básica que comprende el sistema examinado (incluyendo interfaces y medio de comunicación) debe ser identificada. Por ejemplo, los elementos de un entorno de red de computadoras incluirán los hosts, los componentes de la red, interfaces y cualquier otra entidad perteneciente a la arquitectura. Si no se identifica la arquitectura completa en este paso, entonces las vulnerabilidades en los componentes extraños pueden no ser detectadas en los siguientes pasos del proceso.

Existen diferentes técnicas para especificar la arquitectura del sistema; "una de ellas podría describir y hacer un diagrama de los componentes e interconexiones de un sistema dado. Dicha especificación estructural es importante porque provee información sobre el ambiente que rodea cada componente; además, la especificación arquitectónica del sistema debe incluir una descripción de las propiedades funcionales de los componentes e interfaces del sistema, con lo que se provee una vista más lógica de la arquitectura y puede identificarse la interacción que existe entre los diferentes componentes del mismo"[22].

Además, la especificación arquitectónica debe incluir información relacionada a la prioridad relativa de los diferentes elementos de la arquitectura, lo que requiere la identificación del propósito básico o la misión de la arquitectura. Los elementos críticos serán los que, si se remueven, impedirán que se cumpla la misión del sistema.

[22] Amoroso, Edward. 1994. Ed. Prentice-Hall. "Fundamentals of Computer Security Technology".

Finalmente, la especificación arquitectónica debe incluir una descripción de cualquier mecanismo de seguridad existente que ha sido instalado previamente como un medio para reducir las amenazas detectadas. En algunos casos, el resultado del proceso de ingeniería de seguridad del sistema será que dichos mecanismos son inadecuados o innecesarios. En otros casos más raros, el resultado del proceso será que los mecanismos son adecuados y no se necesita atención adicional a la seguridad.

b) Identificación de Amenazas, Vulnerabilidades y Ataques

Las amenazas potenciales a un sistema deben usarse en el segundo paso como la base para identificar vulnerabilidades en los componentes y los tipos de ataques que pueden ser desarrollados aprovechando estas vulnerabilidades. Generalmente, la identificación de amenazas de alto nivel involucra una amplia estimación del daño potencial que puede ser causado con respecto a los componentes básicos que comprenden los elementos arquitectónicos.

c) Estimación del Riesgo

El riego estimado debe ser calculado para todos los componentes de la arquitectura utilizando las prioridades estimadas y la identificación de amenazas, vulnerabilidades y ataques como los parámetros principales en la fórmula del riesgo.

"El riesgo estimado para un componente dado se incrementará conforme mayor sea el daño potencial al sistema y disminuirá con el incremento de la dificultad para un atacante malicioso. Así, si un sistema puede ser dañado potencialmente de forma seria y es fácil para un intruso causar tal daño, entonces el riesgo estimado se considera como alto. Si, por otro lado, el daño potencial del sistema no es considerable y los intrusos no tienen facilidades para provocar tal daño, entonces el riesgo será estimado como bajo"[23].

Nótese que el proceso de ingeniería de seguridad del sistema puede terminar con la estimación del riesgo; esto es, puede ser que el riesgo estimado sea considerado como aceptablemente bajo. De cualquier forma tal determinación afectará enormemente los propósitos y la misión del sistema.

d) Priorización de Vulnerabilidades

Asumiendo que el riesgo determinado es demasiado alto, el siguiente paso en el proceso involucra la estimación de la prioridad de las vulnerabilidades de los diferentes componentes. Claramente, la estimación del riesgo del paso anterior proveerá un mecanismo directo para establecer esta priorización; esto es, los componentes con el mayor riesgo de seguridad estimado serán clasificados para tener la prioridad más alta desde la perspectiva de la ingeniería de seguridad del sistema.

El paso de priorización es importante ya que provee un medio para establecer un orden para la instalación de las protecciones de seguridad; como resultado, si los recursos

[23] Ídem.

están limitados para instalar protecciones al sistema, entonces primero serán dirigidos a las áreas de mayor prioridad.

e) Identificación e Instalación de Protecciones

En este paso, se identifica un conjunto de mecanismos de protección de seguridad potenciales, los cuales pueden incluir mecanismos y procedimientos de seguridad estándar. Las ventajas y desventajas de cada protección en el contexto del sistema también deben ser examinadas. Las ventajas típicas para buscar un candidato para la protección de seguridad incluyen un impacto mínimo en la utilidad, un impacto mínimo en el rendimiento del sistema, el costo mínimo y el impacto mínimo a los procedimientos y aplicaciones existentes.

Una vez que los mecanismos de protección se han seleccionado de todos los candidatos posibles, deben ser integrados al sistema, dicha integración debe ser realizada de tal manera que no introduzca nuevas vulnerabilidades al mismo. Ésta es una consideración importante porque es posible que al mitigar los efectos de un tipo de amenaza, se introduzca un nuevo tipo de amenaza potencial al sistema.

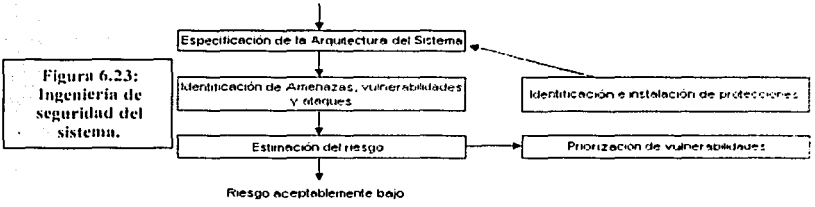


Figura 6.23: Ingeniería de seguridad del sistema.

Nótese que todo el proceso de ingeniería de seguridad del sistema debe repetirse hasta que el riesgo estimado para el sistema sea aceptable (Figura 6.23). A menudo el proceso se repite varias veces para la identificación de vulnerabilidades, estimación del riesgo y la integración de la protección antes de que el riesgo se haya reducido adecuadamente. Además, la iteración del proceso algunas veces sólo requiere que se repita una parte del mismo.

Conclusiones

A través de los capítulos de este trabajo ha podido observarse que instalar un sistema de comunicaciones confiable no es una tarea fácil, ya que son muchos y muy complejos los factores que influyen directamente e indirectamente en el diseño del sistema, por lo que se deben a analizar detalladamente todos los elementos que lo integrarán, así como el grado de seguridad que se desea incorporar, con el objeto de establecer el escenario ideal en el que se implantará el sistema.

Como vimos, para seleccionar el medio de transmisión las consideraciones son bastantes, aparte del costo se deben analizar factores como la distancia, la velocidad de transmisión, el medio ambiente, etc. Además se debe tomar en cuenta que la tecnología LAN y WAN a utilizar influyen directamente en la elección del medio, ya que generalmente se define en función de los requerimientos específicos de cada tecnología.

En el diseño de la red corporativa la selección de las tecnologías adecuadas está en función del tipo de tráfico, es decir de las aplicaciones con que cuenta la organización, así como la cantidad de información que fluye dentro de la misma, por tales motivos es indispensable determinar la cantidad de ancho de banda promedio que se necesitará, especialmente considerando las horas pico, para cubrir adecuadamente las necesidades de comunicación interna (red LAN) y externa (red WAN).

Por otro lado, mantener una red 100% segura hoy en día es prácticamente imposible debido al enorme crecimiento de Internet, ya que este hecho ha provocado que la red corporativa esté expuesta no solo a los posibles ataques del personal que labora en la organización, sino también a cualquier ataque desde cualquier parte del mundo, puesto que conforme se incrementa la cantidad de nodos en Internet, de la misma manera se incrementa la posibilidad de sufrir algún ataque desde el exterior.

Debido a esta situación los mecanismos de seguridad se definen en base a lo que la organización desea proteger, en muchas ocasiones la configuración de un *firewall*, el uso de *NAT* para proteger la red interna o la configuración de *filtros* en los dispositivos de comunicaciones será suficiente para mantener la integridad de la información, sin embargo en ocasiones las *políticas de seguridad* pueden ser más rígidas dependiendo del tamaño de la organización y la cantidad de información y/o equipos que se desean salvaguardar. Es por ello que considero que si se establecen meticulosamente las políticas de seguridad dentro de la entidad es posible, con las herramientas de seguridad disponibles en la actualidad, proteger adecuadamente la información crítica de la empresa.

Cabe señalar que es mucho más fácil diseñar un modelo de seguridad adecuado si se realiza conjuntamente con el diseño del sistema de comunicaciones, puesto que se pueden

definir claramente los puntos criticos de la red y la información que se desea proteger, así como la ubicación de los equipos principales, lo que permite una identificación más precisa de las necesidades de la organización, las cuales son diferentes para cada caso y deben ser cuidadosamente analizadas para implantar la red empresarial y las herramientas de seguridad que mejor se adapten a las necesidades de comunicación de la institución.

Finalmente podemos decir que si se realiza una evaluación detallada de las necesidades de la entidad tomando en cuenta los elementos clave mencionados en este trabajo de investigación (la selección del medio de transmisión, de las tecnologías LAN y WAN y la implantación de los mecanismos de seguridad necesarios) ***sí es posible, en las condiciones tecnológicas actuales, diseñar e implantar una red de comunicaciones de datos funcional que proteja la información crítica de la organización que circula dentro de la red interna y hacia Internet.***

Glosario

Adaptabilidad. Es la cualidad que debe poseer el sistema mediante la cual es capaz de evolucionar dinámicamente con arreglo a su entorno, de manera que atraviesa diferentes estados en los que conserva su eficacia y su orientación el objetivo que constituye su finalidad.

Algoritmo. Dícese del procedimiento para resolver problemas en términos de las acciones a ejecutar o el orden en que se ejecutarán dichas acciones en un problema dado. Conjunto de Instrucciones que especifican la secuencia de operaciones a realizar, en orden, para resolver un sistema específico o clase de problema.

Algoritmo de Cifrado. Sistema de cifrado que permite mover información por las redes telemáticas con seguridad.

Amenaza. Es una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Anagrama. Del griego "anágramma" y el latín "anagramma" (aná=cambio; gramma =escritura). Un anagrama es una palabra o frase obtenida mediante la transposición de las letras de otra palabra o frase, por ejemplo un anagrama de la palabra "letras" sería "lastre".

Ancho de Banda. Cantidad de información, normalmente expresada en bits por segundo, que puede transmitirse en una conexión durante la unidad de tiempo elegida. Rango de frecuencias asignadas a un canal de transmisión.

Antena. Dispositivo que recibe la señal de la unidad central de control y la convierte en una señal radio-eléctrica que es irradiada hacia las unidades terminales de los usuarios en una configuración punto-multipunto.

Anuncio de Ruteo. Proceso en el cual un ruteador envía actualizaciones de ruteo en intervalos de tiempo específicos con el fin de que otros ruteadores en la red puedan mantener una lista de rutas válidas.

Atacante. Persona encargada de efectuar ataques en contra de la seguridad de un sistema.

Ataque. Son acciones encaminadas a descubrir la clave secreta de un criptosistema. Se refiere a cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.

Atenuación. Es la pérdida de energía de una señal conforme se propaga a su destino por un medio de transmisión y se mide en dB y dB/Km.

Autenticación. Dentro de las medidas de seguridad que pueden llegar a implantarse en Internet se tiene ésta que es una verificación de determinado usuario o proceso para tener acceso a cierto sistema, o realizar una operación en específico. Es aplicable también para verificar la identidad de origen de un mensaje.

Backbone. Eje central de una red de computadoras de alta velocidad que distribuye el tráfico de paquetes a otras redes de velocidad inferior.

Banda Base. Transmisión de señales sin modulación. En una red local de banda base, las señales digitales (1 y 0) se insertan directamente en el cable como pulsos de tensión. Todo el espectro del cable es ocupado por la señal. Característica de una tecnología de redes donde solo se utiliza una frecuencia portadora. La red Ethernet es un ejemplo de red banda base.

Bit. Es la unidad de información más pequeña. Puede tener sólo dos valores o estados: 0 ó 1, encendido o apagado. La combinación de estos valores es la base de la informática, ya que los circuitos internos de la computadora sólo son capaces de detectar si la corriente llega o no (1 ó 0). Su nombre proviene de la contracción de las palabras "binary" y "digit" (dígito binario).

Bombas de Tiempo. Son programas ocultos en la memoria del sistema, en los discos o en los archivos de programas ejecutables, por ejemplo archivos con extensión .exe o .com. Esperan una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en la pantalla al llegar el momento de la explosión; llegado el momento se activan cuando se ejecuta el programa que los contiene. Son programas que ejecutan órdenes informáticas destructivas condicionalmente dependiendo del estado de las variables de ambiente, relacionadas con números o con el tiempo.

Bulbo. Primer dispositivo electrónico que permitió la amplificación de señales de radio; tenía los inconvenientes de estar sujeto a desgaste, alto consumo de corriente y voluminosidad, fue sustituido ventajosamente por el transistor.

Bypass. Elemento que permite en un momento dado evitar el paso de la corriente por algunos componentes de un circuito. Uso de las facilidades de transmisión, usualmente para datos, que evita la red de la compañía telefónica local.

Byte (octeto). Dentro de las unidades de medición de memoria en las computadoras un byte representa el conjunto de ocho bits que forman un caracter.

Caballo de Troya. Programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas maliciosas.

Cifrar. Ocultar mediante un procedimiento que permite a un emisor encubrir el contenido de un mensaje o un archivo, de modo que solo las personas que posean una clave determinada puedan accesar a dicha información.

Circuito Integrado. Es un pequeño circuito electrónico utilizado para realizar una función electrónica específica, como la amplificación. Se combina por lo general con otros componentes para formar un sistema más complejo y se fabrica mediante la difusión de impurezas en silicio monocristalino, que sirve como material semiconductor, o mediante la soldadura del silicio con un haz de flujo de electrones.

Circuito Virtual. Servicio de conmutación de paquetes en el que se establece una conexión (circuito virtual) entre dos estaciones al comienzo de la transmisión. Todos los paquetes siguen la misma ruta, no necesitan llevar una dirección completa y llegan secuencialmente a su destino. Circuito lógico diseñado para asegurar una comunicación confiable entre dos dispositivos de red.

Clave de Acceso. Una clave de acceso es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o parte del mismo, a una terminal o computadora personal, un punto en la red, etc. Muchas veces se utiliza la terminología inglesa (*password*) para referirse a la clave de acceso.

Codificación Manchester. Técnica de señalización digital utilizada por el IEEE 802.3 y Ethernet en la que hay una transición en medio de cada intervalo de duración de un bit y se utiliza como señal de reloj. Se codifica un 1 con nivel alto durante la primera mitad del bit; se codifica un 0 con nivel bajo durante la primera mitad del bit.

Codificación Manchester Diferencial. Esquema de codificación digital en que se utiliza la transición a la mitad de la duración del bit para efectos de temporización y una transición al comienzo de cada duración de bit denota un cero. Es el esquema de codificación utilizado por las redes IEEE 802.5 y las redes Token Ring.

Colisión. Situación en la que dos paquetes se transmiten a través de un medio al mismo tiempo; su interferencia hace a ambos incoherentes. En Ethernet, se presenta cuando dos nodos transmiten al mismo tiempo. Las tramas de cada uno de los dispositivos se colisionan y se dañan cuando están en el medio físico.

Conectividad. Capacidad de dos o más elementos hardware o software para trabajar conjuntamente y transmitirse datos e información en un entorno informático heterogéneo.

Conector. "Enchufe" que facilita la unión (conexión) física entre dos dispositivos y, a la vez, la comunicación de datos entre ambos o el intercambio de corriente eléctrica. Se conoce por conector a la terminal de un sistema al que se conectan determinados periféricos.

Confiabilidad. Es la razón entre señales de sobrevivencia esperadas y recibidas en un enlace; si la razón es alta, entonces la línea es confiable. También se la utiliza como una medida de ruteo.

Confidencialidad. Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. Se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan accesar a la información almacenada en él.

Conmutación de Circuitos. Método de comunicación en el que se establece un camino de comunicación entre dos dispositivos a través de uno o más nodos de conmutación intermedios. Sistema de conmutación en el que debe haber una trayectoria de circuito físico dedicada entre el emisor y el receptor durante la "llamada".

Conmutación de Mensajes. Técnica de conmutación que involucra la transmisión de mensajes desde un nodo a otro a lo largo de la red. El mensaje se almacena en cada nodo hasta que esté disponible una trayectoria de ruteo al siguiente nodo.

Conmutación de Paquetes. Método de transmisión de mensajes a través de una red de comunicación en la que los mensajes largos se subdividen en pequeños paquetes. Los paquetes se transmiten después como en conmutación de mensajes. Método de conexión de de redes en el que los nodos comparten el ancho de banda entre sí al enviar paquetes.

Conmutador. Dispositivo electrónico que forma el centro de una red de topología en estrella. Los conmutadores usan la dirección destino de una tabla para determinar la computadora que debe recibirlo.

Conmutador Digital. Una red local con topología de estrella. Usualmente se refiere a un sistema que maneja solo datos, no voz.

Contraseña. Información secreta, en general un grupo de caracteres, utilizada para autenticación.

Convergencia. Es la velocidad y habilidad de un grupo de dispositivos de red que corren un protocolo de ruteo específico para llegar a un acuerdo respecto a la topología de una red después de un cambio en dicha topología.

Core. Parte de la red por la que atraviesa el tráfico de las redes externas hacía la red interna y viceversa. Se encuentra en el límite entre la red interne e Internet.

Costo. Suma total de todos los gastos realizados para instalar, mantener y administrar una red de comunicaciones.

Crecimiento. Se refiere al aumento de los nodos y/o computadoras que se encuentran permanente y directamente conectadas a la red de comunicaciones de la organización.

Criptoanálisis. Metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer la técnica utilizada para la criptografía.

Criptoanalista. Persona encargada de efectuar el criptoanálisis.

Criptografía. Este término se forma del vocablo griego kruptos, "oculto" que se traduce como: "Arte de escribir de manera peculiar o de modo esotérico". En computación se refiere a los mensajes que son enviados por un emisor que oculta el contenido del mensaje a manera de que sólo ciertas personas previamente seleccionadas tengan acceso a la información por medio de una clave después de haberla descifrado. Es la ciencia que estudia la manera de cifrar y descifrar los mensajes para que resulte imposible conocer su contenido a los que no dispongan de una determinada clave.

Criptología. La palabra criptología proviene de las palabras griegas Kryto y logos y significa estudio de lo oculto. Una rama de la criptología es la criptografía, que se ocupa del cifrado de mensajes.

Chip. Oblea muy fina de silicio sobre la que se colocan muchos transistores pequeñísimos para formar un circuito integrado.

Datagrama. En conmutación de paquetes es un paquete, independiente de los otros paquetes, que lleva información de ruteo suficiente desde el DTE origen hasta el DTE destino sin la necesidad de establecer una conexión entre los DTE y la red. Es la agrupación lógica de información que se envía como una unidad de la capa de red por un medio de transmisión sin el establecimiento previo de un circuito virtual.

Decibelio. Medida de la intensidad relativa de dos señales. El número de decibelios es 10 veces el logaritmo del cociente de la potencia de dos señales o 20 veces el logaritmo del cociente de tensión de dos señales.

Demultiplexaje. Es la separación de múltiples flujos de entrada que han sido multiplexados en una señal física común para obtener múltiples ráfagas de salida.

Descifrar. Descubrir el contenido de un mensaje o archivo cifrado por un emisor a través de un procedimiento que solo pueden llevarlo a cabo las personas que posean una determinada clave de acceso.

Diafonía. Fenómeno por el que una señal transmitida en un circuito o canal de un sistema de transmisión crea un efecto indeseado en otro circuito o canal.

Disponibilidad. Significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de alguna falla. Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.

E1. Esquema de transmisión digital de área amplia, utilizado principalmente en Europa para transportar datos a una velocidad de 2.048 Mbps. Las líneas E1 se pueden alquilar a las compañías telefónicas para su uso particular.

Encapsulamiento. Es la función de empaquetado de datos en un encabezado particular de protocolos. Por ejemplo, los datos de Ethernet se empaquetan en un encabezado Ethernet específico antes de circular por la red.

Enmascaramiento. Alteración, intencionada o no, que dificulta la compresión de un mensaje.

Escalabilidad. En términos generales, la escalabilidad hace referencia a la capacidad del sistema para mantener y/o mejorar su rendimiento medio conforme aumenta el número de clientes.

Estación Terrestre. Conjunto de equipos de comunicaciones diseñados para recibir señales (y generalmente transmitir a) de satélites.

Fiabilidad. Característica de los sistemas informáticos que determina el tiempo de funcionamiento que transcurre sin que se produzca ninguna falla.

Firewall. Se denomina así al sistema de seguridad que se coloca entre la red local e Internet, de esta manera la empresa o compañía regulará completamente toda la comunicación hacia Internet estableciendo sus políticas de seguridad.

Fragmentación de Paquetes. Técnica utilizada para dividir un datagrama grande en datagramas más pequeños llamados fragmentos. El destino final reconstruye los fragmentos.

Frecuencia. Número de veces que se repite una onda en una cantidad de tiempo determinada. Su unidad de medida es el hertzio y la velocidad de los procesadores (o ciclos de reloj) se mide en megahertzios (MHz). A mayor índice, más velocidad de proceso.

Funcionalidad. Es la cualidad de la red que permite a la organización cumplir con los requisitos laborales para los que fue diseñada.

Hacker. Persona de elevados conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer.

Hardware. Se trata de todos los componentes físicos de una computadora, entre los cuales se pueden mencionar el disco duro, procesador, monitor, etc. que en conjunto con el *software* (programas) hace funcionar una computadora.

Hub. Es un término que se utiliza para describir un dispositivo que sirve como el centro de una red con topología de estrella. Es un dispositivo de hardware o software que contiene múltiples módulos de red y equipo de red independientes, pero conectados. Los hubs pueden ser activos (si repiten las señalen enviadas hacia ellos) o pasivos (si solamente multiplexan las señales que se les envían).

Identificación. Proceso llevado a cabo por un sistema de control de red, mediante el cual se valida la identidad de una línea individual, usuario o aparato que requiere un servicio.

Información. Grados de libertad que existen en una situación específica para elegir entre señales, símbolos, mensajes o patrones a trasmitirse, que permiten la elaboración de un concepto. La información la componen datos que se han colocado en un contexto significativo y útil y se ha comunicado a un receptor, quien la utiliza para tomar decisiones.

Ionosfera. Región de la superficie exterior de la atmósfera hasta una altura de 1.000 Km en la que se concentran los electrones libres producto de la ionización en cantidades suficientes para modificar las características de las ondas de radio que las atraviesan; la ionosfera se divide en 3 regiones principales: la región D, la región E y la región F. La duración, altitud, profundidad y concentración de electrones de la misma varía a lo largo del día, y de estación a estación, y también se ven afectados por otras condiciones cambiantes como actividad de las manchas solares.

Integridad. Se refiere a las medidas de salvaguarda que se incluyen en un sistema de información para evitar la pérdida accidental de los datos.

Intercepción. Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora.

Interfaz. Se denomina así a la zona de contacto o conexión entre dos elementos de hardware, lo mismo se ocupa para dos aplicaciones o entre un usuario con una aplicación.

Internet. Se denomina así a la red de telecomunicaciones que surgió en los Estados Unidos en 1969 y que en sus orígenes era de carácter meramente militar, para el día de hoy convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural, económico, etc. Se puede clasificar en tres niveles: el primero lo conforman las redes troncales, el segundo las redes de nivel intermedio y el tercero lo constituyen las redes aisladas. El Internet es además una red multiprotocolo capaz de soportar cualquier tecnología.

Longitud de Onda. Es la distancia mínima entre dos puntos con el mismo valor de la perturbación (se toman como referencia los picos). Es, por tanto, una distancia, con lo que su unidad de medida es el metro. Es la distancia que recorre el pulso mientras una partícula del medio que recorre la onda realiza una oscilación completa.

Métrica. Es el método que permite a un algoritmo de ruteo determinar que una ruta es mejor que otra; esta información se guarda en tablas de ruteo.

MHz. Equivalente a 1.000 KHz ó 100.000 Hz. Unidad de medida que se aplica con frecuencia en informática para especificar la velocidad de proceso del CPU.

Microondas. Ondas electromagnéticas en el rango de frecuencias entre 2 y 40 GHz.

Modulación. Proceso por el que se modifican algunas de las características de una oscilación y onda de acuerdo con las variaciones de otra señal llamada generalmente

moduladora. Proceso, o resultado del proceso, de variación de algún parámetro de una señal, llamada portadora, de acuerdo con una señal mensaje. Es el proceso por el cual las características de las señales eléctricas se transforman para representar información.

Multicast. La red copia un solo paquete de datos y lo envía a un subconjunto específico de direcciones en la red (comunicación uno a varios).

Multiplexaje. Concepto general que se refiere a la combinación de fuentes independientes de información, de manera que puedan transmitirse por un sólo canal de comunicación. El multiplexaje ocurre tanto en el hardware (es decir, pueden multiplexarse las señales eléctricas) como en el software (es decir, el software de protocolo puede aceptar mensajes enviados por varios programas de aplicación y luego enviarlos por una sola red a varios destinos).

Multiplexor. Dispositivo que toma datos a baja velocidad procedentes de varias terminales o computadoras y los convierte en un flujo único, lo que permite transmisiones simultáneas a alta velocidad.

Nanómetro. Es la mil millonésima parte de un metro, 1nm = 0.000000001 metros.

Negación de Servicio. Significa que los usuarios no pueden obtener del sistema los recursos deseados. Acción de impedir el acceso, estando autorizado, a recursos o retrasar las operaciones.

Ohm. Se define como la resistencia eléctrica de un elemento pasivo en un circuito eléctrico que es recorrido por una corriente continua de un ampere cuando se aplica a sus terminales una tensión eléctrica en corriente continua de un volt. Se expresa en términos de las unidades de base de masa, longitud, intensidad de corriente eléctrica y tiempo.

Omnidireccional. La propagación y emisión de una señal desde una antena en todas direcciones.

Ondas de Radio. Ondas electromagnéticas que se extienden en parte del espectro que va de las altas frecuencias de radio audibles, justo un poco debajo de la región infrarroja.

Overhead. Desperdicio de ancho de banda, causado por la información adicional (de control, secuencia, etc.) que debe viajar, además de los datos, en los paquetes de un medio de comunicación. Afecta el rendimiento de una conexión.

Palmtop. Se trata de una innovación dentro del ámbito de las computadoras, su tamaño es muy pequeño y cabe en la palma de la mano, entre otras funciones, sirve como agenda y proporciona la conexión a Internet.

Paquete. Grupo de bits que incluyen datos e información adicional de control; generalmente se refiere a una unidad de datos del protocolo del capa de red (capa 3 del modelo OSI). Es la agrupación lógica de información que incluye un encabezado que contiene información de control y datos de usuario.

Permutación. Es una ordenación de los elementos de un conjunto dado. Ejemplo: sean 3 números cualesquiera, {1,2,3}, se entiende por permutación de esos 3 números a las distintas formas en que se puede ordenar ese conjunto. De esta forma se puede decir que este conjunto tiene las siguientes permutaciones: {1,2,3}, {1,3,2},{2,3,1}, {2,1,3}, {3,1,2}, {3,2,1}.

Protocolo. Directrices que regulan las comunicaciones entre computadoras. Descripción formal de un conjunto de reglas y convenciones que rigen el modo en que los dispositivos de una red intercambian información.

Protocolo de Ruteo. Es un protocolo que logra el direccionamiento de paquetes a través de la implantación de un algoritmo de ruteo específico. Entre los ejemplos de protocolos de ruteo se incluyen IGRP, OSPF y RIP.

Protocolo ruteable. Protocolo que puede ser direccionado a través de un equipo de ruteo: este equipo debe ser capaz de interpretar la red lógica como lo especifica el protocolo ruteable. Algunos ejemplos de protocolos ruteables son: AppleTalk, IP e IPX.

Radiación. La radiación puede definirse como energía en tránsito de un lugar a otro.

Radiación Electromagnética. Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos. La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas).

Red. Grupo de máquinas interconectadas físicamente entre sí que utilizan software que les permite compartir dispositivos e intercambiar información.

Red de *Campus*. Es una red extendida que ofrece interconectividad a varios edificios dentro de un mismo predio privado, habitualmente espacios universitarios.

Red perimetral. Red que se encuentra entre la red protegida y la red interna con el objetivo de agregar una capa adicional de seguridad.

Relay. Dispositivo en la terminología OSI que conecta dos o más redes o sistemas de redes. En la capa de enlace de datos (Capa 2), un relay es un puente; en la capa de red (Capa 3), un relay es un ruteador.

Rendimiento. Tasa de la información que llega a, y posiblemente a través de de, un punto en particular en un sistema de red.

Retardo. Es el tiempo entre el inicio de la transmisión de un emisor y la primera respuesta recibida por éste. Es el tiempo que se requiere para transferir un paquete desde una fuente a un destino por una trayectoria determinada.

Router. Dispositivo físico o lógico que garantiza la conexión entre nodos y redes bajo diversos protocolos; se encarga de que los paquetes de datos lleguen a su destino.

Ruido. Señales no deseadas que se combinan con la señal de transmisión o de recepción y que por lo tanto la distorsionan.

Ruta Redundante. Es el empleo de dos o más caminos o vías para alcanzar un destino, con el fin de asegurar la continuidad del servicio. Es la provisión de caminos alternos para los casos en que la ruta principal esté sobrecargada o no disponible.

Ruteador de Frontera. Dispositivo de ruteo ubicado en el límite de la red interna y externa.

Satélite. Artefacto puesto en órbita alrededor de la Tierra o de otro cuerpo del espacio; es empleado para reflejar información, o como medio de comunicación.

Satélite Geoestacionario. Satélite geosincrónico cuya órbita circular y directa se encuentra en el plano ecuatorial de la Tierra y que, por consiguiente, aparenta estar fijo; la deriva existente es mínima, cuenta con motores de apogeo y perigeo que corrigen dicha deriva y la órbita en la que se desliza está localizada aproximadamente a 36.0000 Km. de la tierra en un plano ecuatorial.

Seguridad Informática. Es la estructura de control establecida para gestionar la disponibilidad, integridad, confidencialidad y consistencia de los datos, sistemas de información y recursos informáticos. Es un conjunto de controles que tienen la finalidad de mantener la confidencialidad, integridad y confiabilidad de la información.

Servicios no Orientados a la Conexión. Término que describe la transferencia de datos sin un circuito virtual. Los servicios no orientados a conexión carecen de las tres etapas existentes en los servicios orientados a la conexión y en este caso, los interlocutores envían todos los paquetes de datos que componen una parte del diálogo por separado, los cuales pueden llegar a su destino en desorden y por diferentes rutas. Es responsabilidad del destinatario ensamblar los paquetes, pedir retransmisiones de aquellos que se dañaron y darle coherencia al flujo recibido.

Servicios Orientados a la Conexión. Término que se utiliza para describir la transferencia de datos que requiere el establecimiento de un circuito virtual. Es un tipo de servicio en el que obligatoriamente debe establecerse una conexión o camino entre el origen y el destino antes de que cualquier dato pueda transmitirse. Los servicios orientados a conexión se caracterizan porque cumplen tres etapas en su tiempo de vida: negociación del establecimiento de la conexión (etapa 1), sesión de intercambio de datos (etapa 2) y negociación del fin de la conexión (etapa 3).

Servidor *Proxy*. Es un servidor muy particular que se encarga de centralizar el tráfico entre Internet y una red independiente, de manera que evita que cada una de las computadoras que conforman esa red independiente disponga de manera innecesaria de una conexión

directa a Internet. Además utiliza mecanismos de seguridad como (firewall) que evita accesos no autorizados desde Internet hacia la red independiente.

Sincronización. Establecimiento de una temporización común entre el emisor y el receptor.

Sistema Operativo. Conjunto de programas fundamentales sin los cuales no sería posible hacer funcionar la computadora con los programas de aplicación que se desee utilizar. Sin el sistema operativo, la computadora no es más que un elemento físico inerte.

Switch. Dispositivo de red que filtra, envía e inunda de frames en base a direcciones MAC. El switch opera en la capa de enlace de datos del modelo OSI. Es un término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

T1. Instalación de transporte digital en una WAN. Un T1 transmite datos formateados en DS-1 a una velocidad de 1.544 Mbps a través de la red telefónica conmutada.

Tarjeta de Red. Es una tarjeta que proporciona capacidades de comunicación en la red hacia y desde un sistema de computación; también se conoce como *adaptador de red.*

Telecomunicaciones. Comunicaciones de datos por medios electrónicos. Es el intercambio de información usando módems, líneas telefónicas u otros dispositivos electrónicos.

Telemática. Simbiosis o combinación de *informática, electrónica* y *comunicaciones.* Este término fue acuñado por primera vez en 1978 por Simón Nora y Alan Minc. Se considera como los servicios de transmisión de información orientados al usuario.

Temporizador. Pequeño circuito integrado que poseen todas las placas base de las computadoras y que hace la función de generar frecuencias programables; se encarga, entre otras cosas, de actualizar el reloj interno del sistema varias veces por segundo.

Terminal de Abonado. Se entiende por terminal de abonado aquel equipo telefónico a instalarse en el extremo remoto de una línea telefónica (vista desde la central de conmutación) y que permite la recepción y/o transmisión de mensajes vocales, escritos o de datos.

Texto Cifrado. Texto resultante de aplicar un procedimiento de cifrado a un texto plano.

Texto Plano. Texto o señales con significado propio en el idioma o código público que se emplee en cada caso.

Token. Término utilizado para referirse a un derecho, por ejemplo el derecho a transmitir, que se intercambia entre los usuarios de una facilidad de telecomunicaciones para asegurar un uso ordenado de la facilidad y para controlar el diálogo. Es un frame que contiene sólo información de control; la posesión del token permite a un dispositivo de red la transmisión de datos.

Topología. Estructura, que consta de caminos y conmutadores, que proporciona el medio de interconexión entre los nodos de la red. Es el arreglo físico de los nodos y el medio de transmisión dentro de una estructura de red corporativa.

Topología de Anillo. Topología de red que consiste en una serie de repetidores conectados entre sí a través de enlaces de transmisión unidireccionales para formar un único ciclo cerrado; cada estación se conecta a la red a través de un repetidor. Aunque conectadas de manera lógica en forma de anillo, físicamente suelen estar organizadas como una estrella de ciclo cerrado.

Topología de Estrella. Topología LAN en la que los puntos terminales de la red se conectan a un switch central común a través de enlaces punto a punto. Una topología de anillo que está organizada como estrella, implanta una estrella unidireccional de ciclo cerrado, en lugar de enlaces punto a punto.

Topología en Malla. Topología de red en la que cada nodo de la red se conecta con cada uno de los nodos que integran la red.

Topología Horizontal. Conocida también como topología de bus es una arquitectura lineal de LAN en la cual los envíos desde las estaciones de la red se propagan a todo lo largo del medio y son recibidos por todas las demás estaciones.

Topología Jerárquica. Conocida también como topología vertical o topología de árbol es una topología LAN similar a una topología horizontal, excepto porque las redes con topología jerárquica pueden contener ramas con nodos múltiples. Los envíos desde una estación se propagan por el medio y son recibidos por todas las demás estaciones.

Tráfico. Conversaciones o comunicaciones telefónicas en curso; número de circuitos telefónicos en uso durante determinado tiempo. Es el conjunto de peticiones de comunicación emanadas de un grupo de circuitos o de enlaces considerados, tomando en cuenta tanto el número de las comunicaciones como sus duraciones. Técnica de dar curso a los mensajes que ingresan a un sistema de conmutación.

Tráfico de *Broadcast*. La transmisión de datos se realiza por un sólo canal de comunicación compartido por todas las máquinas de la red. Cualquier paquete de datos enviado por una máquina es recibido por todas las demás. Un broadcast consiste en enviar paquetes de datos a todos los nodos de un segmento de red; el tráfico de broadcast puede afectar el rendimiento de dicha red. Para direccionar un mensaje a todas las máquinas se usa una dirección de broadcast que es reconocida por todas las máquinas dentro de la red en la cual todos sus bits son iguales a 1.

Tráfico *Ruteado*. Es el proceso de encontrar una ruta hacia un detsino en específico. Es el movimiento de un paquete desde un origen hacia un destino. El ruteo ocurre en la capa 3 del modelo OSI.

Tráfico *Switcheado*. Es la acción de mover un paquete (o frame) de un puerto a otro. El switcheo ocurre en la capa 2 del modelo OSI.

Trama. Grupo de bits que incluye datos, además de una o más direcciones y otra información de control de protocolo. Generalmente se refiere a la unidad de datos del protocolo de la capa de enlace (capa 2 del modelo OSI). Es la agrupación lógica de información enviada como una unidad de la capa de enlace de datos a través de un medio de transmisión. Con frecuencia se refiere al encabezado y delimitador, utilizados para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad.

Transceiver. Dispositivo que recibe la potencia de un sistema mecánico, electromagnéntico o acústico y lo transmite a otro, generlamente en forma distinta. El microfono y el altavoz son ejemplos de transceivers. En comunicaciones es un transmisor/receptor de señales de radio frecuencia, sirve para convertir señales de un medio de transmisión dado a otro distinto a diferentes velocidades.

Transistor. Dispositivo electrónico activo en el cual se aprovechan las propiedades de un semiconductor y que es capaz de realizar las mismas funciones de las válvulas termoelectrónicas o tubos termoiónicos, con las ventajas de ser de dimensiones reducidas en relación con estos y de tener un gasto de energia insignificante, por no necesitar corriente de caldeo o calefacción. Es un elemento amplificador de corriente, basado en el diferencial de conducción de la corriente por electrones y huecos: el material utilizado para su construccion es por lo general germanio o silicio con cantidades pequeñas y controladas de ciertas impurezas.

Transmisión Analógica. Transmisión de una señal a través de cables ò por medio del aire, en la que se transporta la información a través de la variación de alguna combinación de la amplitud, frecuencia o fase de la señal.

Transmisión Asíncrona. Es el tipo de comunicación por la cual los datos se pasan entre dispositivos de forma asíncrona o sea que la transmisión de un caracter es independiente del resto de los demás caracteres. El patrón seguido es: caracter de comienzo + caracteres de datos + caracter de parada.

Transmisión Digital. Es el proceso de enviar información como una secuencia de digitos binarios, toda vez que dicha información se ha convertido en una serie de pulsos eléctricos binarios que pueden asumir uno de dos posibles valores (0 ó 1).

Transmisión en Paralelo. Transmisión de datos que se realiza entre dos dispositivos octeto a octeto o sea de 8 en 8 bits a la vez.

Transmisión *Full-Duplex*. Comunicación de datos que se mantiene bidireccionalmente y que visualiza en la pantalla de la computadora que los envía los caracteres enviados al sistema remoto. Dicho sistema o host deberá desactivar el eco local (echo off) ya que si no visualizará dos veces seguidas el mismo caracter.

Transmisión *Half-Duplex*. Comunicación de datos mantenida bidireccionalmente pero no simultáneamente sino sucesivamente (una computadora tras otra) y cuyos caracteres

enviados al sistema remoto se visualizan en la pantalla de la computadora que los envía. El sistema remoto o "host" deberá activar el eco local (echo on) ya que si no no visualizará ningún caracter.

Transmisión Serial. Transmisión de datos que se realiza entre dos dispositivos bit a bit, uno después del otro.

Transmisión *Simplex*. Transmisión de datos solamente en una dirección preasignada.

Transmisión Síncrona. Es el tipo de comunicación por la cual los datos se pasan entre dispositivos de forma síncrona o sea que la transmisión depende de la meticulosa sincronización de los datos transmitidos, enviados y de sus propios mecanismos de transmisión. No requiere un caracter de comienzo ni un caracter de parada a diferencia de la comunicación asíncrona.

Transponder. Parte de un satélite que tiene como función principal la de amplificar la señal que recibe de la estación terrena, cambiar la frecuencia y retransmitirla nuevamente a una estación terrena, con una cobertura amplia. Equipo receptor y emisor que al recibir una señal radioeléctrica (llamada señal de interrogación) transmite automáticamente una señal de característica generalmente diferente a la de la primera señal de respuesta.

Tubo de vacío. Véase bulbo.

Unicast. Es el envío de un paquete de un host a otro dentro de la red (comunicación uno a uno).

Velocidad de transmisión. Velocidad a la que puede transferirse la información a través de un puerto.

Virus. Se le llama así a todo programa computacional que se duplica a sí mismo dentro de un sistema y que se añade a otros programas que se utilizan ocasionando fallas. En la actualidad son la principal preocupación de los usuarios que navegan en Internet, en donde tienen su mayor campo de acción.

Vulnerabilidad. Debilidad en la seguridad de un sistema de información. Puede ser: 1) Explotable. Vulnerabilidad que puede ser explotada en la práctica para romper un objetivo de seguridad. 2) Potencial. Vulnerabilidad supuesta que puede ser utilizada para romper un objetivo de seguridad, pero cuya posibilidad, explotación o existencia no ha sido aún demostrada.

ABM	Asynchronous Balanced Mode
AC	Access Control
ACK	Acknowledgment
ACL	Access Control List
ANSI	American National Standards Institute
ARM	Asynchronous Response Mode
ARQ	Automatic Repeat Request
ASCII	American Standard Code for Information Interchange
AT&T	American Telephone and Telegraph Company
BC	Committed Burst Size
BE	Excess Burst Size
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
CBC	Cipher Block Chaining
CCITT	International Consultative Committee on Telegraphy and Telephony
CDMA	Code Division Multiplexing
CFB	Cipher FeedBack
CIR	Committed Information Rate
C/R	Command/Response field bit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DAS	Dual Attachment Station
DBS	Direct Broadcast Satellite
DCE	Data Circuit-terminating Equipment
DE	Discard Eligibility Indicator
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DISC	Disconnect
DLCI	Data Connection Identifier
DM	Disconnected Mode
DMA	Direct Memory Access
DNS	Domain Name System
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
EA	Address Extension
EBCDIC	Extended Binary-Coded Decimal Interchange Code
ECB	Electronic CodeBook
ED	End Delimiter

EIA	Electronic Industries Association
EISA	Extended Industry Standards Architecture
FC	Frame Control
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FECN	Forward Explicit Congestion Notification
FRAD	Frame Relay Assembler/Disassembler
FRMR	Frame Reject
FRND	Frame Relay Network Device
FS	Frame Status
FTP	File Transfer Protocol
GFI	General Format Identifier
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
ILD	Injection Laser Diode
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunications Union
LAN	Local Area Network
LAP-B	Link Access Procedure-Balanced
LCI	Logical Channel Identifier
LEC	Local Exchange Carrier
LED	Light Emitting Diode
LLC	Logical Link Control
MAC	Media Access Control
MCA	Micro Channel Architecture
MIS	Management Information System
MSAU	Multistation Access Unit
NAT	Network Address Translation
NBS	National Bureau of Standards
NFS	Network File System
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NRM	Normal Response Mode
OFB	Output FeedBack
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAD	Packet Assembler/Disassembler
PBS	Public Broadcasting Service
PBX	Private Branch Exchange
PCM	Pulse Code Modulation

PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PVC	Permanent Virtual Circuit
RAM	Random Access Memory
RD	Request Disconnect
REJ	Reject
RFC	Request For Comments
RIM	Request Initialization Mode
RIP	Routing Information Protocol
RNR	Receive Not Ready
RR	Receive Ready
RSA	Rivest, Shamir and Adlman
RS-233	Recommended Standard 232
SA	Source Address
SABM	Set Asynchronous Balanced Mode
SABME	Set Asynchronous Balanced Mode Extended
SARM	Set Asynchronous Response Mode
SARME	Set Asynchronous Response Mode Extended
SAS	Single Attachment Station
SD	Star Delimiter
SIM	Set Initialization Mode
SNRM	Set Normal Response Mode
SNRME	Set Normal Response Mode Extended
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Start of Frame Delimiter
SREJ	Selective Reject
STDM	Statistical Time Division Multiplexing
STP	Shielded Twisted Pair
SVC	Switched Virtual Circuit
TCP/IP	Transmission Control Protocol / Internet Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
UA	Unnumbered Acknowledged
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UI	Unnumbered Information
UP	Unnumbered Poll
UTP	Unshielded Twisted Pair
VC	Virtual Circuit
VHF	Very High Frequency
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WWW	World Wide Web
XID	Exchange identification

Bibliografía

1. Amoroso, Edward. Fundamentals of Computer Security Technology. Ed. Prentice-Hall. United States of America, 1994.
2. Black, Uyless. Redes de Computadoras, Protocolos, Normas e Interfaces. Ed. AlfaOmega. 2ª edición. México, 1997. 585 pp.
3. Cisco Systems, Inc. Academia de Networking de Cisco Systems: Guía del Primer Año. Ed. Pearson Educación, S. A. 2ª edición. Madrid, España, 2002. 736 pp.
4. Cisco Systems, Inc. Academia de Networking de Cisco Systems: Guía del Segundo Año. Ed. Pearson Educación, S. A. 2ª edición. Madrid, España, 2002. 702 pp.
5. Comer, Douglas E. Redes Globales de Información con Internet y TCP/IP. Ed. Prentice-Hall. 3ª edición. México, 1996. 621 pp.
6. Collin, Serge. Computer, Interfaces and Communications. Ed. Prentice-Hall International. París, France, 1990.
7. De Alarcón Álvarez, Enrique. Diccionario de Informática e Internet. Ed. Anaya multimedia. Madrid, España, 2000. 347 pp.
8. Ferreyra Cortés, Gonzalo. Virus en las Computadoras. Ed. Macrobit. 2ª edición. México, 1993. 155 pp.
9. Ford, Merilee. Tecnologías de Interconectividad de Redes. Ed. Prentice-Hall. México, 1998. 716 pp.
10. Gratton, Pierre. Protección Informática. Ed. Trillas. México, 1998. 272 pp.
11. Herrera Pérez, Enrique. Introducción a las Telecomunicaciones Modernas. Ed. Limusa. México, 1998. 410 pp.
12. Ibarra Quevedo, Raúl y Serrano López, Miguel A. Principios de Teoría de las Comunicaciones. Ed. Limusa. 1ª reimpresión. México, 2001. 321 pp.
13. Nombela, José Juan. Seguridad Informática. Ed. Paraninfo. España, 1997. 258 pp.
14. Ramos, Emilio y Schroeder, Al. Concepts of data Communications. Ed. Macmillan Publishing Company. United States of America, 1994. 249 pp.
15. Ramteke. Networks. Ed. Prentice-Hall. 2nd edition. United States of America, 2001. 705 pp.
16. Rodríguez G., Jorge E. Introducción a las Redes de Área Local. Ed. McGraw-Hill. México, 1996. 157 pp.
17. Servin, Claude. Telecommunications: Transmission and Network Architecture. Ed. Springer. England, 1999. 233 pp.
18. Stallings, William. Comunicaciones y Redes de Computadoras. Ed. Prentice-Hall. 6ª Edición. Madrid, España, 2000. 776 pp.
19. Varios Autores. CCNP "Cisco Certified Network Professional". Cisco LAN Switch Configuration Study Guide. Ed. McGraw-Hill. United States of America, 1999. 612 pp.
20. Varios Autores. LAN TIMES. Guía de Redes de Área Extensa. Ed. McGraw-Hill. 1ª edición en Español. Madrid, España, 1997. 469 pp.
21. Varios Autores. LAN TIMES. Guía de Seguridad e Integridad de Datos. Ed. McGraw-Hill. 1ª edición en Español. Madrid, España, 1998. 342 pp.
22. Varios Autores. Técnicas Criptográficas de Protección de Datos. Ed. Alfaomega. 2ª edición. Madrid, España, 2001. 372 pp.

Referencias WWW

1. http://atenea.udistrital.edu.co/cursos/mt.redesl/grp02/indice.html
2. http://rinconquevedo.iespana.es/rinconquevedo/Criptografia/criptografia.htm
3. http://www.antel.com.uy/instalaciones_domiciliarias/NETTAT009_120400.pdf
4. http://www.cita.es/textos/glosar.htm
5. http://www.funtel.org/3_DOCUMENTOS_DISPONIBLES/3_doc_disp_contenido/3al_Glosarios/3al_glosarios_contenido/3al1_glosario%20de%20terminos/3al1_glosario_palabras/
6. http://www.geektools.com/rfc/rfc1631.txt
7. http://www.info-ab.uclm.es/asignaturas/42602/cortafuegos.pdf
8. http://www.lasalle.edu.co/esi_cursos/informatica/termino/seguridad_informatica.htm
9. http://www.mmcicom.com/mmcicom/tutorial/fddi.html
10. http://www.openbsd.org/faq/pf/es/nat.html