Facultad de Contaduría y Administración

Sistema de Universidad Abierta

Apuntes
SISTEMAS DE TELECOMUNICACIONES

Profesor: L.A. Salvador Meza Badillo

Índice

I. MODELO OSI

OSI (Interconexión de Sistemas Abiertos), conocido como modelo de referencia OSI, describe cómo 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.
OSI es un modelo conceptual compuesto de siete capas; en cada una de ellas se especifican funciones de red particulares. Fue desarrollado por la ISO (Organización Internacional de Estándares) en 1984, y actualmente se considera el modelo principal de arquitectura para la comunicación entre computadoras.

Capas OSI

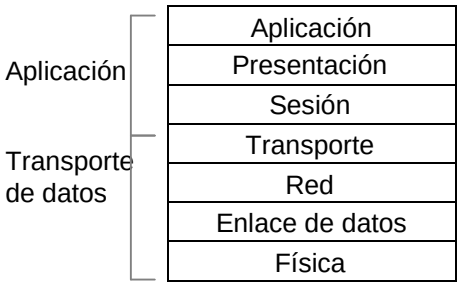
OSI divide las funciones implicadas en la transferencia de información entre computadoras de red, en siete grupos de tareas más pequeñas y fáciles de manejar. A cada una de las siete capas se asigna una tarea o grupo de tareas. Cada capa es razonablemente individual, por lo que las tareas asignadas a cada capa se pueden actualizar sin afectar a las demás.
La lista siguiente detalla las siete capas del modelo OSI:

- Capa 7—Capa de aplicación
- Capa 6—Capa de presentación
- Capa 5—Capa de sesión
- Capa 4—Capa de transporte
- Capa 3—Capa de red
- Capa 2—Capa de enlace de datos
- Capa 1—Capa física

7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Características de las capas OSI

Las siete capas del modelo de referencia OSI se pueden dividir en dos categorías: capas superiores y capas inferiores.
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. Tanto los usuarios como los procesos de la capa de aplicación interactúan con aplicaciones de software que contienen un componente de comunicación.
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. La capa inferior, la física, que es la más cercana al medio de transmisión de la red física (el cableado de la red, por ejemplo), es la responsable de colocar la información en el medio de transmisión.



Protocolos

El modelo OSI, proporciona un marco conceptual para la comunicación entre computadoras, pero el modelo en sí mismo no es un método de comunicación. La comunicación real se hace posible al utiliza protocolos de comunicación.
Un *protocolo* es un conjunto formal de reglas y convenciones que gobierna el modo en que las computadoras intercambian información por un medio de transmisión de red. Hay una gran variedad de protocolos: protocolos LAN, protocolotes WAN, protocolos de red y protocolos de ruteo.
Los protocolos LAN operan en las capas físicas y de enlace de datos del modelo OSI y definen la comunicación a través de los diferentes medios de transmisión. Los protocolos WAN operan en las tres capas inferiores del modelo OSI y definen la comunicación a través de los diferentes medios de transmisión de área amplia. Los protocolos de ruteo son protocolos de la capa de red responsables de la determinación de la trayectoria y la conmutación del tráfico. Los protocolos de red son los diferentes protocolos de las capas superiores que están en un grupo determinado de protocolos.

Interacción entre las capas del modelo OSI

Por lo general una capa determinada del modelo OSI se comunica con otras tres capas OSI: la capa ubicada directamente debajo de ella y su capa equivalente en otro sistema de computadoras en red.

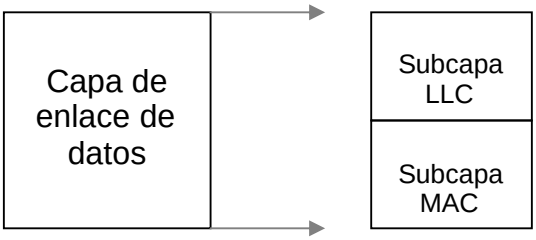
Capa física

Está capa define las especificaciones eléctricas, mecánicas, de procedimientos 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.

Capa de enlace de datos

Proporciona el tránsito confiable de datos a través del enlace de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes características de red y protocolo, incluyendo el direccionamiento físico, topología de red, la notificación de error, la secuencia de tramas y el control de flujo. El direccionamiento físico define cómo 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. La notificación de error de 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 más tráfico del que pueda manejar simultáneamente.

El IEEE (Instituto de Ingenieros en Electrónica y Electricidad) ha subdividido la capa de enlace de datos en dos subcapas: LLC (Control de Enlace Lógico) y MAC (Control de Acceso a Medios).



La subcapa LLC de la capa de enlace de datos administra las comunicaciones entre los dispositivos unidos por un enlace individual de red. La subcapa LLC está definida en la especificación IEEE 802.2 y soporta los servicios orientados y no orientados a la conexión.
La subcapa MAC de la capa de enlace de datos administra el protocolo de acceso al medio de transformación 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.

Capa de red

Esta capa proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos al combinarse en una red. Esto se logra a través del direccionamiento lógico. Soporta servicios orientados y no orientados a la conexión de los protocolos de las capas superiores.
Los protocolos de la capa de red son los protocolos de ruteo, y también otro tipo de protocolos están implementados en la capa de red.

Capa de transporte

Implementa servicios confiables de datos entre redes, transparentes a las capas superiores. Entre las funciones habituales de la capa de transporte se cuentan el control de flujo, el multiplexaje, la administración de circuitos virtuales y la verificación y recuperación de errores.
El control de flujo administra a la transmisión de datos entre dispositivos para que el dispositivo 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. Es la capa de transporte la que 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 datos para resolver cualquier error que pudiera ocurrir.
Algunas implementaciones de la capa de transporte incluyen el protocolo de control de transmisión, el protocolo de enlace de nombres y protocolos de transporte estándar OSI. TCP (Protocolo de Control de Transmisión) es el protocolo en el conjunto TCP/IP que proporciona una transmisión confiable de datos.

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 en diferentes dispositivos de red. Estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión.

Capa de presentación

Brinda una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema se legible por la capa de aplicación de otro sistema.

Los formatos de presentación de datos comunes o el uso de formatos estándares de video, sonido e imagen, permiten el intercambio de datos de aplicación entre diferentes tipos de sistemas de computadoras. Los esquemas de conversión utilizan para intercambiar información entre sistemas utilizando diferentes presentaciones de texto y datos, como EBCDIC y ASCII.

Capa de aplicación

Esta es la capa de OSI más cercana al usuario final, lo cual significa que tanto la capa de aplicación de OSI como el usuario interactúan de manera directa con la aplicación de software.
Esta capa interactúas con las aplicaciones de software que implementan un componente de comunicación. Dichos programas de aplicación están fuera del alcance del modelo OSI. Las funciones de la capa de aplicación incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de 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 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.

Servicios de red orientados y no orientados a la conexión

En general, los protocolos de conectividad de redes y el tráfico de datos que soportan se pueden caracterizar como orientados a la conexión. El manejo de datos orientados a la conexión implica el uso de una trayectoria específica que se establece durante el tiempo que dura la conexión establecida en forma permanente.
El servicio orientado a la conexión tiene tres fases: el establecimiento de la conexión, la transferencia de datos y la terminación de la conexión.
Durante la *fase del establecimiento de la conexión*, se determina una sola trayectoria entre los sistemas origen y destino. De hecho, los recursos de la red se reservan en este momento para asegurar un grado de servicio constante, es decir un rendimiento eficiente global garantizado.
En la *fase de transferencia de datos,* los datos se transmiten en forma secuencial por la trayectoria que se ha establecido. Los datos siempre llegan al sistema destino en el orden que fueron enviados.
Durante la fase de terminación de la conexión, se termina una conexión establecida que ya no se vaya a utilizar. Si se requiriera más comunicación entre los sistemas origen y destino, sería necesario establecer una nueva conexión.
Los servicios orientados a la conexión, son muy útiles para la transmisión de datos de aplicaciones que no toleran retardos y secuenciación de paquetes. Las aplicaciones de voz y video se suelen basar en servicios orientados a la conexión.
El servicio no orientado a la conexión tiene dos importantes ventajas respecto al servicio orientado a la conexión: la sección dinámica de la trayectoria y la asignación dinámica del ancho de banda. La selección dinámica de la trayectoria permite que el tráfico sea ruteado de modo que evite su paso por fallas de red.
Los servicios no orientados a la conexión son muy útiles en la transmisión de datos de aplicaciones que pueden tolerar cierta cantidad de retardo y resecuenciación. Las aplicaciones de datos se basan en servicios no orientados a la conexión.

II. FUNDAMENTOS DE LAS TELECOMUNICACIONES

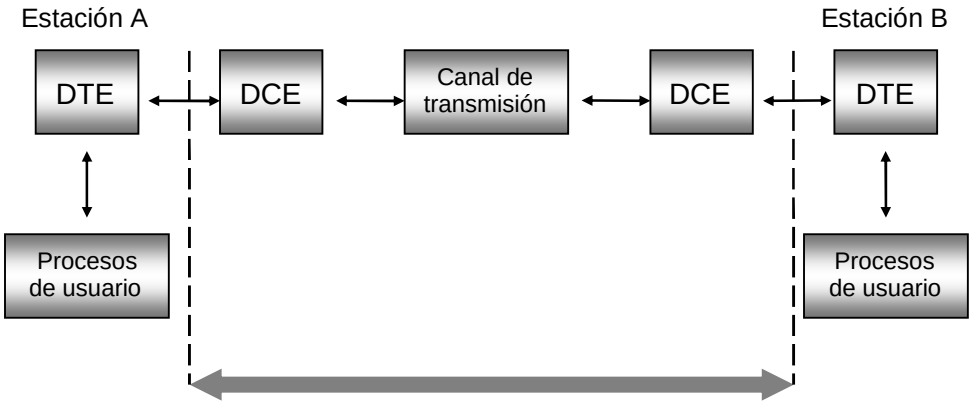
Etimológicamente, telecomunicaciones proviene de las raíces: *tele* (distancia) y *comunicare* (compartir), esto es compartir a distancia. En el sentido moderno, telecomunicaciones es la transmisión por medios electrónicos de sonido, datos, facsímiles, imágenes, voz, video y cualquier otra información, empleando medios analógicos y/o digitales.

Modelo Básico de las telecomunicaciones

Medio de transmisión

Los tres elementos básicos que integran un sistema de comunicaciones son: fuente o emisor, destino o receptor y finalmente el medio de transmisión que bien puede ser alámbrico o inalámbrico.

Modelo básico de un sistema de comunicaciones



Medio de transmisión

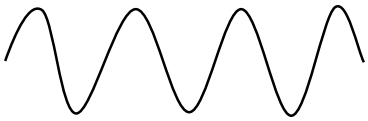
DTE: Equipo Terminal de Datos, es donde se generan y procesan las tareas e información del usuario.

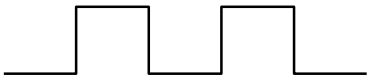
DCE: Equipo de Comunicación de Datos, es un equipo utilizado para conectar, establecer, mantener y terminar una conexión, además realiza cualquier tipo de conversión de señales, codificación y demás procesos requeridos por el DTE, el ejemplo más común de un DCE es el módem.

Dependiendo de la aplicación, y desde el punto de vista del usuario, el medio de transmisión puede o no incluir el equipamiento DCE.

Tipos de señales

Señales analógicas ***Señales digitales***





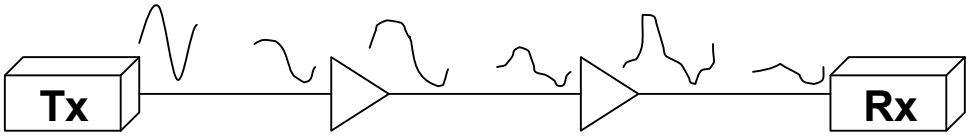
Una señal eléctrica es una forma de energía que nos representa información (generalmente adquirida de un equipo transductor como el micrófono). Las señales pueden clasificarse de muchas formas:

Las de naturaleza analógica, que representan instantáneamente la información de la fuente a través de valores continuos de amplitud en el tiempo (como pasa en una conversación telefónica en donde el micrófono produce señales eléctricas que corresponden a las variaciones en la energía sonora)

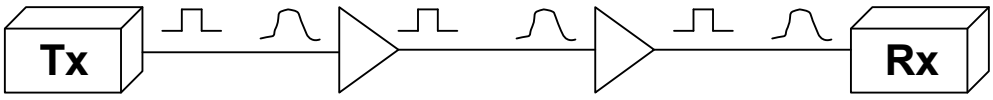
Las señales digitales, que son discretas en el tiempo y en amplitud; esto significa que la amplitud sólo puede tomar uno de dos valores 0 ó 1 en intervalos definidos de tiempo.

SEÑALES ANALÓGICAS	**SEÑALES DIGITALES**
- SUCEPTIBLE AL RUIDO E INTERFERENCIA	- CONVIVENCIA CON SISTEMAS DIGITALES (CD-ROM, STEREO, ETC.)
- PRESENTAN GRANDES ATENUACIONES EN GRANDES DISTANCIAS	- ES POSIBLE LA REGENERACIÓN
- NO ES POSIBLE REGENERARLAS	- SENSIBLES A LA SINCRONÍA
	- SENSIBLES AL RETARDO
	- ES POSIBLE LA CODIFICACIÓN
	- DETECCIÓN Y CORRECIÓN DE ERRORES

TRANSMISIÓN



ANALÓGICA



DIGITAL

Características de las señales

Las señales pueden tener formas muy caprichosas, sin embargo, todas ellas pueden representarse como la combinación de varias señales de tipo periódico cuyas características son más sencillas de analizar:
Amplitud (A): La intensidad máxima de la señal o valor pico, puede ser representada en valores de voltaje o corriente, etc.

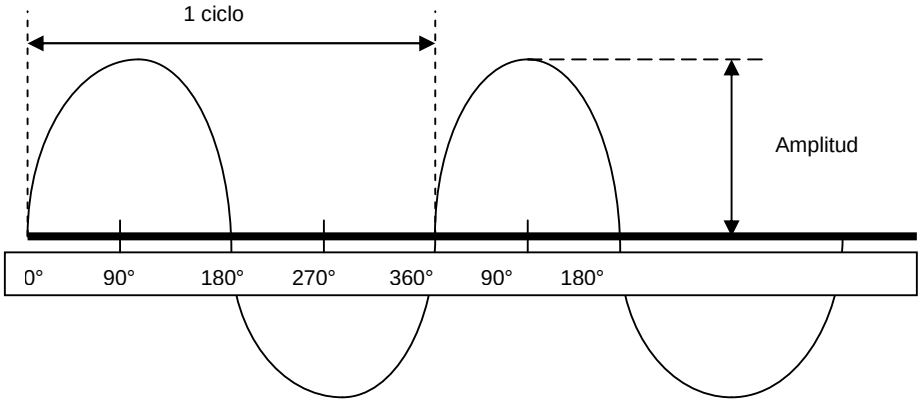
Período (T): Tiempo que tarda en cumplirse un ciclo, se mide en segundos.

Frecuencia (f): Número de ciclos en la unidad de tiempo, su unidad es el Hertz que es la unidad inversa de los segundos, por lo que $f = 1 / T$

Fase (q): Ángulo de la señal, se mide en grados o bien en radianes.

Diferencia de Fase: La diferencia de fase o ángulo de desfasamiento, indica el ángulo que se encuentra atrasada o adelantada con respecto a otra señal.

Longitud de onda (λ): Distancia que cubre la señal en un ciclo, utilizamos los metros como unidad de medida. La forma de calcular su valor resulta si dividimos la velocidad de la luz entre la frecuencia, así $\lambda = v / f$.



Ancho de banda

Es la diferencia entre las frecuencias máxima y mínima de una señal.
Ancho de banda vs. capacidad del canal: La tasa máxima de transmisión de un canal se conoce como capacidad del canal y tiene como unidades a los bits por segundo (bps).

Modos de operación

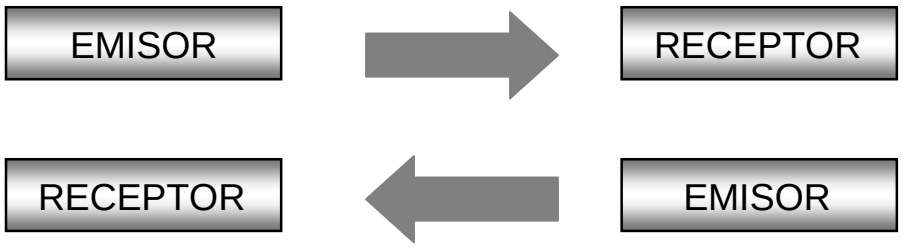
La comunicación emisor-receptor puede tener varios modos de operación dependiendo de las limitaciones del medio de transmisión, de los equipamientos DCE y DTE y de los procesos del usuario.

Simplex

Medio de transmisión

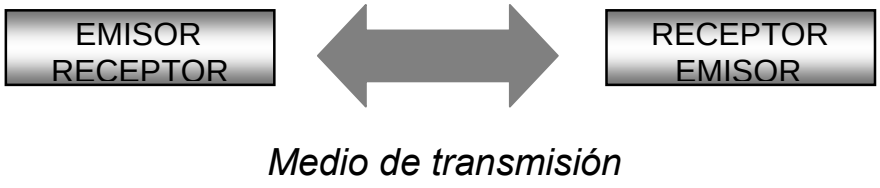
Simplex: En el modo de operación simplex, la comunicación es unidireccional, esto es, mientras un equipo transmite el otro sólo recibe; en ningún momento el receptor puede tomar el papel de emisor, un ejemplo de este tipo de modo de operación es la TV. En este caso, no es el medio de transmisión el que impone el tipo de operación, sino el diseño de la aplicación.

Half Duplex



Half Duplex: La comunicación Half Duplex es bidireccional, pero no en forma concurrente. A comparación del modo simplex, ambos nodos pueden fungir como receptor y emisor pero nunca de manera simultánea, sino que tienen que invertir sus roles. El ejemplo más simple de este tipo de comunicación es el walkie talkie.

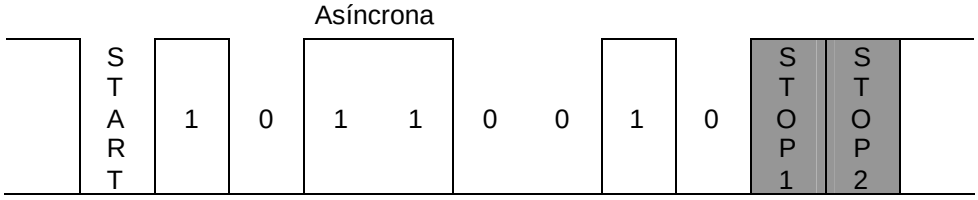
Full Duplex



Full Duplex: En el modo Full Duplex, ambos nodos pueden transmitir y recibir de manera simultánea. Ejemplo de este modo lo encontramos en las redes switcheadas y equipos de videoconferencia.

Modos de flujo

Si tomamos en cuenta la forma en que se sincronizan el receptor y el transmisor, la transmisión puede ser:



Transmisión asíncrona: Fue la primera en ser usada, está orientada a carácter y tiene un alto overhead. Existen bits de paro y de inicio.

La característica principal de esta transmisión es que no hay necesidad de que el emisor y receptor compartan el mismo pulso de reloj.

Transmisión síncrona:. Se elimina el bit de paro y de inicio, es necesario que el emisor y receptor sincronicen sus relojes

Conmutación

La conmutación es la técnica utilizada para la transferencia de información entre dos máquinas. Existen dos clasificaciones:

Conmutación de circuitos: Su uso se presenta principalmente con tráfico de voz y utilizan conmutación pura por lo que:

Ofrecen un circuito dedicado desde el origen hasta el destino a través de los nodos intermedios, reservándole un ancho de banda a lo largo de toda la trayectoria (se utilice o no, por lo que se puede presentar subutilización del medio). Los nodos intermedios o DCE's fungen como conmutadores y no poseen dispositivos de almacenamiento (buffers).

La comunicación requiere del establecimiento previo de la ruta a través de la dirección (un número telefónico por ejemplo) e información de disponibilidad y prioridades.

En los sistemas modernos, los circuitos dedicados son virtuales, es decir, sobre un mismo medio físico se tienen varios de estos circuitos y de acuerdo con la utilización del medio, se pueden aplicar algoritmos de comprensión, supresión de silencios, redireccionamiento de tráfico y similares para optimizar los recursos de la red.

Conmutación de paquetes: Se emplea principalmente con tráfico de datos y hacen uso de la conmutación y almacenamiento, por lo que:

Cuando un equipo desea enviar información a otro, éste agrega al mensaje la dirección del equipo destino y lo pasa a la red para que los DCE's intermedios definan su encaminamiento. Los DCE's (ruteadores) con base en la información de tráfico, disponibilidad, costos e información de rutas, deciden la ruta óptima hacia el siguiente DCE (próximo salto) o éste a su vez realiza los mismo hasta llegar al nodo de destino. Si existe tráfico, los DCE's proporcionan almacenamiento temporal (buffers) para manejo de picos de tráfico.

Conmutación de paquetes

Encabezado: *Dirección > Origen*
Origen > Dirección

El equipo que envía la información debe incluir su dirección y la del destino en cada paquete enviado, esto trae un decremento en el desempeño, pues el encabezado representa información adicional. Para asegurar un desempeño óptimo es necesario procurar que el tamaño del encabezado sea mínimo con respecto a la cantidad de información. Además, los encabezados de cada paquete son procesados y modificados por cada nodo de la red en su trayectoria, lo cual genera retardos adicionales en el flujo de información.
La clasificación que se le de a una transmisión dependerá de la forma de operar de los DEC's involucrados.

Una red de conmutación puede ser de dos tipos:
Conmutación pura: En este tipo, primero se establece una trayectoria (PATH) del nodo fuente al destino, ésta se cerrará cuando la comunicación haya concluido. A este tipo de redes también se le conoce como orientadas a conexión.

Conmutación y almacenamiento: En este tipo de redes, también conocidas como “Store & Forward”, los mensajes recibidos son analizados para decidir su próximo “salto”, además pueden ser almacenados temporalmente si el medio de transmisión presenta congestión.

Modulación

La modulación de señales consiste en modificar las características de una señal portadora para adecuarla a las características del medio de transmisión.
Las telecomunicaciones modernas utilizan gran cantidad de medios para la transmisión de información. El audio, de tipo analógico, es transmitido en la radio por señales analógicas; mientras que las redes de datos emplean estas mismas señales (analógicas) para transmitir información digital como en el caso de los enlaces de microondas.
Al adecuar las características de las señales a las del medio de transmisión se logran varios objetivos, entre los cuales tenemos: la cobertura geográfica (distancia) y la inmunidad al ruido.

Existen dos tipos básicos de modulación: analógica y digital.
Modulación analógica: Este tipo de modulación se ocupa en la transferencia de información analógica a través de señales analógicas. Es el tipo de modulación más conocido por la antigüedad de su uso.

Existen tres técnicas básicas para modulación analógica:

Modulación de Amplitud (AM)

Modulación de la frecuencia (FM)

Modulación de la fase (PM)

La transmisión de señales a bajas frecuencias (debajo de los 30KHz) resulta muy costosa por la potencia requerida para el transmisor (para lograr largas distancias) y el tamaño de las antenas, entre otras razones, por lo que las señales dentro de estos rangos normalmente se realizan a altas frecuencias con la finalidad de “portar” eficientemente estas señales a su destino. Las aplicaciones principales de este tipo de modulación las encontramos en radiodifusión.

Modulación digital: Este tipo de modulación se ocupa en la transferencia de información digital a través de señales analógicas.

Surge de la necesidad de transferir información digital por las líneas telefónicas (uso de módem).

Existen tres técnicas básicas para modulación analógica:

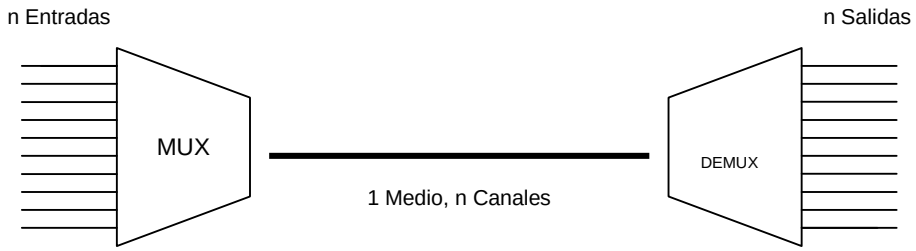
En amplitud o ASK (Amplitude-Shift Keying)

En frecuencia o FSK (Frecuency-Shift Keying)

Fase o PSK (Phase-Shift Keying)

> Las señales digitales poseen formas de onda cuadradas con significado de 0 ó 1. Si este tipo de ondas se transfieren por medios analógicos, la señal cuadrada se distorsionaría y el receptor no tendría información suficiente para interpretarla. Debido a esto, las señales son transformadas para su transporte en medios analógicos.

Multiplexaciópn o multicanalización



Técnica para permitir que **n** cantidad de mensajes o señales compartan un solo medio de transmisión.

Las dos principales técnicas de multiplexación son:

Multiplexación por división de tiempo TDM (Time Division Multiplexing): Se emplea generalmente en transmisiones digitales, por lo que es utilizado en los enlaces WAN de las redes de datos y transmisión de voz digital. Divide la capacidad de canal por intervalos de tiempos.

Existen muchas variantes de TDM como:

ATDM (Asyncronous TDM)

STDM (Stadistical TDM)

STM (Synchronous Transfer Mode)

Multiplexación por división de frecuencias FDM (Frecuency Division Multiplexing): Es la técnica para transmisiones analógicas, todas las señales se transmiten al mismo tiempo por diferentes rangos de frecuencias.

Redes de computadoras

Es un conjunto de equipos de cómputo interconectados entre sí para compartir recursos e información.

Ventajas:

- Información no centralizada.
- Mejora la seguridad y control de la información.
- Expande las capacidades de un equipo.
- Comunica a los usuarios de los diferentes equipos.
- Reduce o elimina duplicidad de trabajo.
- Permite acceder a información en menos tiempo.
- Reduce costos.
- Globalización.
- Productividad.

Clasificación:

Por extensión geográfica: Es difícil establecer los límites entre las diferentes clasificaciones geográficas, debido a que algunas de éstas poseen características en común con alguna otra. Una forma de auxiliarse para clasificarlas es por medio de los tipos de dispositivos utilizados dentro de una y otra.

LAN (Local Area Network): Son las más comunes. Usualmente tienen varios servidores operando en el mismo segmento de red. Su rango de velocidad es de 4 Mbps. Ej. Red con servidor NT.

MAN (Metropolitan Area Network): Diseñadas para proveer altas velocidades de comunicación dentro de una diudad. La mayoría usa líneas provistas por una compañía de transporte (carrier, E1's). Diseñadas para agrupar LAN's y pueden ser más lentas o rápidas que éstas. Son más pequeñas que la WAN pero se compensan en rapidez.

WAN (Wide Area Network): Abarcan grandes áreas, tales como los nodos metropolitanos de la Red UNAM, una ciudad completa, un estado o un país. Incluyen equipo de ruteo para interconectar

redes a través de los enlaces remotos (microondas, E1's). Así mismo, poseen un menor ancho de banda que las LAN, en el orden de Kbps.

También existen otras subclasificaciones (como CAN, DAN, GAN)
CAN (Campus Area Network): Conectan nodos (o posiblemente LAN's) desde múltiples sitios que pueden llegar a estar separados por distancias considerables. A diferencia de una WAN, no utiliza líneas públicas para comunicaciones remotas. Conecta redes a través de cables, fibra o cicroondas. Su rango de velocidad es de 10 Mbps a 622 Mbps.

DAN (Departamental Area Network): Término usado principalmente en ambientes de oficinas para interconectar grupos pequeños de computadoras y compartir recursos. Ej. Red de Windows 95.

GAN (Global Area Network): Redes de Tecnología Internetworking que integran diferentes países. Ej. Internet.

Por topología: La topología de una red es el patrón de interconexión entre los nodos que la componen. De manera específica, la topología de una red se refiere al modo en que los equipos que la integran están físicamente interconectados; sin embargo, también podemos hablar de una topología lógica, que es el modo en que cada equipo ve e interactúa con la red. El mejor ejemplo de porqué es necesario de hablar de una topología lógica lo tenemos en las redes tipo Ethernet, ya que éstas han evolucionado de un sistema de cableado de bus lineal a uno de estrella, manteniendo un control del flujo de la información basado en un bus lineal (lógico).
En los sistemas inalámbricos no existen conexiones físicas, pero aún así se emplea el término topología para describir la(s) trayectorias (s), ya sea física(s) o lógicas(s), en la(s) que se transfiere la información para que los nodos se comuniquen entre sí.

Lógica: Se refiere a la forma en que la información fluye a través de la red.

Física: Describe cómo el cable conecta a los nodos.

Las topologías básicas son las siguientes:
Anillo: Todos los nodos están conectados el uno con el otro, formando una cadena o círculo cerrado. En algunas implantaciones cada nodo trabaja como un repetidor activo, y en otras es un elemento pasivo. En las implantaciones de repetidor activo, cuando un nodo falla, la continuidad del anillo se interrumpe y todo el sistema se paraliza, en la implantación pasiva, existen elementos adicionales que garantizan una tolerancia a fallas de los nodos.

Bus: Todos los nodos están conectados a un cable central, llamado "bus". A diferencia de la topología de anillo, si un nodo falla, la red continuaría funcionando, pero si se presenta un problema en el bus, todo el sistema deja de trabajar.

Estrella: En esta configuración todos los nodos terminales están conectados a un elemento central, si uno de los nodos terminales falla, esto no afecta a los demás, sin embargo, si el elemento central presenta problemas la red completa deja de funcionar.

Malla: En una configuración de malla, la existencia de múltiples rutas físicas de comunicación entre dos nodos, garantiza una alta disponibilidad. En una configuración de malla completa, cada nodo de la red requiere al menos un enlace con cada uno de los otros nodos. Conforme el número de nodos aumenta; la cantidad de enlaces necesarios también crece, pero geométricamente, esto eleva considerablemente los costos y no siempre garantiza un uso eficiente de cada enlace.

Otras clasificaciones: A continuación se enuncian:

Públicas: Una red pública puede ser definida como aquella creada con fines comerciales y para cubrir necesidades de terceros, con objeto de que cualquier persona o compañía pueda conectarse y hacer uso de ésta.

Internet: Es un conjunto de redes autónomas que se comunican a través del protocolo TCP/IP. Tiene una cobertura global, emplea una gran variedad de tecnologías que hacen posible que todos sus usuarios se comuniquen y usen los servicios que las otras redes ofrecen.

Red Telefónica Pública Conmutada: Mecanismo concebido principalmente para transportar voz. Actualmente consta de medios digitales y analógicos para transferir información.

Privadas: Una red privada se refiere a aquellas redes de datos diseñadas para cubrir las necesidades propias de una empresa o compañía más que con fines de lucro. De las características importantes de las tecnologías de internet es que son independientes de la arquitectura, es decir, se puede hacer uso de éstas desde diferentes plataformas de hardware y software.

Intranet: Red que utiliza tecnología Internet situada detrás de un firewall, para uso exclusivo de empleados de una compañía.

Extranet: Es una Intranet expandida donde se puede acceder a la información por empleados y clientes de la compañía (los externos necesitan validación a través de password).

III. TECNOLOGÍAS DE CONECTIVIDAD EN REDES DE VOZ Y DATOS

Toda comunicación y/o transmisión de datos requiere de un transmisor, un receptor y un medio de comunicación, este último puede ser de diferentes tipos aún cuando la forma de transmitir los datos sea la misma. Por ejemplo, si dos personas entablan una conversación esta puede ser usando el idioma como forma de transmisión pero el medio de comunicación puede ser el aire, por carta, por señales luminosas, etc. Lo mismo pasa en las redes, la transmisión puede ser comúnmente por:
Medios de transmisión guiados, confinados o alámbricos:

- Cable coaxial
- Cable trenzado
- Fibra óptica

Medios de transmisión no guiados, no confinados o inalámbricos:

- Microondas terrestres
- Microondas satelitales
- Radiodifusión
- Ondas de luz

Al seleccionar un medio de comunicación, deben considerarse los siguientes aspectos:

- Tipo de red
- Distancia
- Costo de instalación del cable, conectores y accesorios
- Estructura del edificio
- Costo de mantenimiento
- Ancho de banda (Cantidad de información que puede trasmitirse por un medio)
- Grado de tolerancia a interferencias electromagnéticas
- Atenuación (Pérdida de energía a lo largo de un cable)
- Posibilidades de expansión

Medios de transmisión guiados

Se les considera guiados o confinados porque la señal esta “atrapada” o en confinamiento dentro de un cable mientras que los medios inalámbricos las señales no tienen guía y viajan libres por el espacio, de hecho en la actualidad hay tal cantidad de señales yendo y viniendo, que si no fueran invisibles estaríamos a oscuras cubiertos por todas ellas.
En los 80’s las redes estaban conectadas en su mayoría por cable coaxial que ahora ha sido sustituido por el cable trenzado el cual a su vez será sustituido por la fibra óptica y tecnologías inalámbricas en la medida que los costos bajen y la tecnologías se perfeccionen.
La siguiente tabla tomada de la referencia 1 ofrece un breve resumen de los distintos tipos de cables:

TIPO DE CABLE	ANCHO DE BANDA	LONGITUD MAXIMA	COSTO
Par trenzado Categoría 5	Entre 10Mbps y 100Mbps	100 metros	Bajo
Coaxial fino	10Mbps	185 metros	Bajo
Coaxial grueso	10Mbps	500 metros	Alto
Fibra óptica	De 100Mbps a más de 2Gbps	2 kilómetros	Alto

Cable coaxial

Tiene las siguientes características generales:
Es redondo y consta de un hilo central de cobre rodeado por un aislante de espuma dieléctrica. El aislante está rodeado por otro material conductor formado por una malla trenzada y ésta a su vez está recubierta por un material aislante.

Su auge fue en los años 70 y 80 sin embargo actualmente se usa para transmisión de señales de televisión privada y de banda ancha a través de la tecnología conocida como cable módem.

Usa topología de bus donde las computadoras se conectan a un segmento principal por el cual viaja la señal a través de todos los nodos de extremo a extremo.

Si se produce un corte o una conexión defectuosa en cualquier lugar del bus, la red se divide en dos segmentos que no pueden comunicarse entre sí, y la falta de terminación en uno de los extremos de cada segmento genera perdida de señal y la consecuente caída de la red.
La tarjeta de red va conectada a un conector en forma de T los cuales se conectan al cable coaxial y en los extremos del cable se debe colocar un terminador para cerrar el circuito (resistencia de carga)

El costo de instalación es elevado

Es muy confiable, duradero e inmune a interferencias.

Tiene 2 variedades: coaxial delgado y coaxial grueso

Tipo de cable	Diámetro	Impedancia	Atenuación	Conectores	Aplicación
RG-8/U	0.405”	50 Ω	1.9	N	Ethernet gruesa
RG-58 A/U	0.195”	50 Ω	4.5	BNC	Ethernet delgada
RG-62 A/U	0.242”	93 Ω	2.7	BNC	ARCnet
RG-59 /U	0.242”	75 Ω	3.4	F	TV por cable

Cable Coaxial Delgado:
Su especificación ethernet es 10BASE2, es decir que proporciona una velocidad de transmisión de 10Mbps, utiliza transmisión en banda base y se puede llegar a tender hasta los 200 metros. (referencia 5)

Es más fácil de instalar y resulta más barato que el grueso.

Se pueden conectar hasta 30 nodos

Utiliza conectores T en cada nodo lo que obliga a cortar el cable.

Especificaciones Ethernet del cable coaxial delgado 10BASE2 (Referencia 5)

Especificación	Valor
Longitud máxima de un segmento	185 metros
Número máximo de nodos por segmento	30
Distancia mínima entre nodos	0.5 metros
Número máximo de segmentos	5
Número máximo de repetidores	4
Longitud total máxima con repetidores	925 metros
Impedancia	50 Ohmios

Cable Coaxial Grueso:
Su núcleo es más grande que el coaxial delgado

Su especificación ethernet es 10BASE5, es decir proporciona una velocidad de transmisión de 10Mbps, utiliza transmisión en banda base y se puede llegar a tender hasta los 500 metros (referencia 5)

Es difícil de manejar y debe mantenerse un radio mínimo cuando se realizan curvas, debido al diámetro central del conductor central. (referencia 5)

Se pueden conectar hasta 100 nodos

Utiliza cables AUI por cada nodo lo que evita cortes en el cable.

Especificaciones Ethernet del cable coaxial grueso 10BASE5

Especificación	Valor
Longitud máxima de un segmento	500 metros
Número máximo de nodos por segmento	100
Distancia mínima entre nodos	2.5 metros
Número máximo de segmentos	5
Número máximo de repetidores	4
Longitud total máxima con repetidores	2,500 metros
Impedancia	50 Ohmios

Cable par trenzado

Tiene las siguientes características generales:
Sus inicios fueron en la telefonía con categoría 1 de 2 hilos

Dependiendo de la categoría, contienen de 2 a 8 pares de hilos de cobre aislados y torcidos entre si para evitar interferencias electromagnéticas

Fue aprobado en los 90 por la IEEE y actualmente es uno de los más comunes.

Utilizan conectores RJ-45 que son más baratos que los de coaxial y provocan menos fallos

Es más flexible que el coaxial y por lo tanto es más fácil de instalar

El ancho de banda depende del grosor del cable, de la distancia que recorre y del trenzado.

Básicamente existen 2 tipos de cable de par trenzado, apantallado (STP) y sin apantallar (UTP), aunque este último es el más común, también existió el FTP (Foil Twister Pair) cuya característica era que tenía un alambre o lamina llamado foil que se usaba para aterrizar el cable.

Cable de par trenzado apantallado STP (Shielded Twister Pair):
Fue definido por IBM para las redes Token ring

Está formado por pares de cables de cobre retorcidos en pares y envueltos por un material que los aísla de las interferencias electromagnéticas y de radiofrecuencia llamada pantalla que a la vez está cubierta por una capa de plástico.

La pantalla puede ser de lámina o de filamentos trenzados y es propenso a romperse si se dobla el cable demasiado.

Cuando la pantalla se conecta a tierra, convierte el ruido ambiente en una corriente eléctrica que crea campos magnéticos que se oponen al ruido exterior. El balance de los campos magnéticos es delicado. Si no son exactamente opuestos, la corriente de apantallamiento puede interpretarse como ruido y distorsionar las señales transmitidas por el cable. Esto significa que todos los componentes de conexión deben estar correctamente apantallados.(referencia 3)

Son más caros y difíciles de instalar.

El estándar TIA/EIA-T568-A solo reconoce dos de estos tipos de cable: El 1ª de 2 pares de hilos para uso en cableado vertical y horizontal y el 6ª para latiguillos.

Especificaciones Ethernet del cable de par tranzado apantallado 10BASE-T

Especificación	Valor
Longitud máxima de un segmento	100 metros
Número máximo de nodos por segmento	2
Distancia mínima entre nodos	3 metros
Número máximo de segmentos	1024
Número máximo de segmentos con nodos	1024
Número máximo de concentradores encadenados	4
Impedancia	150 Ohmios

Cable de par trenzado sin apantallar UTP (Unshielded Twister Pair):
Pueden utilizarse en varios tipos de redes como Token ring y Ethernet

Son baratos y fáciles de instalar

No tiene ningún material que sirva de blindaje entre los pares torcidos y el revestimiento exterior del cable

Especificaciones Ethernet del cable de par tranzado sin apantallar 10BASE-T

Especificación	Valor
Longitud máxima de un segmento	100 metros
Número máximo de nodos por segmento	2
Distancia mínima entre nodos	3 metros
Número máximo de segmentos	1024
Número máximo de segmentos con nodos	1024
Número máximo de concentradores encadenados	4
Impedancia	100 Ohmios

Categorías del Cable par trenzado
Los organismos de normalización, como el EIA/TIA, asignan categorías a ciertos tipos de cables, en el caso del par trenzado se le otorga una clasificación por categorías que define su capacidad.

Cat	Hilos	Frec.	Vel.	Norma	Especificación	Aplicaciones
1	2	0 Mhz	4 Mbps			Telefonía de voz, antiguos servicios de telefonía; sistemas de alarma
2	2	1 Mhz	4 Mbps			Telefonía de voz; terminales de minicomputadoras y mainframes IBM; ARCnet; LocalTalk
3	2	16 Mhz	16 Mbps	ANSI/EIA/TIA/ 568-A ISO/IEC 11801 NMX-1-236-NYCE UL 444	10 BASE T (IEEE 802.3) 4/16 Mbps Token Ring (IEEE 802.5)	Telefonía de voz
4	4	20 Mhz	20 Mbps			Token ring a 16 Mbps
5 y 5e	8	100 Mhz	100 Mbps o 1000 Mbps	ANSI/EIA/TIA 568-A y B ISO/IEC 11801 NMX-1-236-NYCE UL 444	10 BASE T (IEEE 802.3) 4/16 Mbps Token Ring (IEEE 802.5) 100 Mbps TP-PMD (ANSI X3T9.5) 100 BASE-VG (100 BASE-NE)	100BASE-TX; OC-3 (ATM); SONet 1000 BASE-T (Gigabit Ethernet)
6	8	200 Mhz	1000 Mbps	ISO/IEC 11801 A ICEA S90-661		

Actualmente la categoría más común es la 5 aunque las nuevas redes cableadas con UTP se están inclinando a la categoría 6 que está siendo cada vez más barata y accesible.

Los cables UTP categoría 5, 5e y 6 tienen el mismo aspecto pero todos los cables de marcas reconocidas tienen impreso en el forro a que categoría pertenecen y como se ve en el cuadro tienen 8 hilos trenzados por pares con los colores verde/verde blanco, naranja/naranja blanco, azul/azul blanco y café/café blanco. Dado que tienen la capacidad de transmitir voz video y datos, 2 pares son para la transmisión de datos (1 par para transmitir y 1 par para recibir), 1 par (el de en medio) para telefonía y 1 par para otros usos como video. La siguiente figura muestra el orden que deben tener los hilos de acuerdo a su color según los estándares TIA/EIA/568ª y 568B los cuales forman parte de un conjunto de estándares que rigen la instalación de cableado estructurado.

Fibra óptica

Características generales:

Están hechas con variados materiales

1. Fibra óptica de vidrio. Tiene el menor nivel de atenuación y tanto el núcleo como el recubrimiento implican una alta pureza óptica, por estar fabricados de dióxido de silicio o de cuarzo fundido. Para incrementar los índices de refracción, se mezcla con algunas impurezas de germanio, titanio o fósforo; tiene el costo más elevado.
2. Fibra óptica de plástico. Tiene la atenuación más alta de todos los tipos de fibra, por lo que se recomienda para redes de corta distancia. El núcleo está hecho de plometilmetacrilato (PMMA) recubierto de un fluoropolímero, además de que su proceso de fabricación es más barato.
3. Fibra óptica de plástico – silicio (PCS). Su atenuación se ubica entre la fibra óptica de vidrio y la de plástico. El núcleo es de vidrio y el recubrimiento de un polímero plástico con menor refracción. Por su estructura, es más difícil la instalación de conectores en este tipo de fibra, lo que la hace la menos popular de las tres.

- Consta de un cilindro de vidrio central revestido por un tubo de vidrio llamado revestimiento.
- El núcleo central y el revestimiento están envueltos por una funda de PVC.
- El tamaño del cable se mide en micras y varia dependiendo del tipo (monomodo o multimodo)
- El núcleo transporta los pulsos de luz originados por dispositivos de diodos emisores de luz (LED) o por un láser.
- El revestimiento de vidrio está diseñado para reflejar la luz y que ésta vuelva al núcleo.
- Los cables compuestos pueden contener de 8 hasta 24 hilos en una misma funda.
- Su principal uso es en el backbone de las redes o para conexiones entre edificios debido a su gran ancho de banda y su baja atenuación.
- Es caro y difícil de instalar
- Es usada en Fast ethernet (100BASE-FX), Gigabit ethernet (1000BASE-FX), Token ring, FDDI, ATM y 100VG-AnyLAN
- Bajas pérdidas (atenuación baja) (típicamente 0.3 dB/km, lo que supone casi un orden de magnitud respecto de un cable coaxial), de forma que es posible transmitir las señales a larga distancia sin necesidad de repetidores o poner estos muy separados entre ellos
- Usa conectores ST dobles o sencillos
- Gran capacidad para transmitir datos debido a la elevada frecuencia de la portadora (en el dominio óptico, típicamente en torno a 190 THz)
- Inmunidad frente a interferencias electromagnéticas radiaciones, por lo que no es preciso apantallamiento electromagnético. Esta inmunidad incluye los pulsos electromagnéticos producidos por explosiones nucleares (aunque la radiación alfa y beta altera las características de transmisión de la fibra)
- No se radia energía fuera de la fibra. Esto dificulta las escuchas no deseadas.
- Son dieléctricas, lo que asegura el aislamiento eléctrico del cable y permite su empleo y manipulación sin peligro en instalaciones de alta tensión. Tanto es así que en la actualidad las empresas de telecomunicación emplean fibras ópticas arrolladas a los conductores de tierra de las líneas de alta tensión de la red de transporte de energía eléctrica.
- Bajo peso
- Las señales contienen poca potencia
- No hay diafonía entre fibras adyacente

Los cables de fibra óptica están disponibles en múltiples configuraciones, los cables simples contienen un hilo de fibra, mientras que los cables duplex contienen dos hilos paralelos en una misma funda. Ambas se pueden utilizar para el cableado ya que los estándares lo permiten pero además del costo la diferencia más importante es el grosor del núcleo.

Longitud de onda en nm	Características de Transmisión en Fibras Ópticas				
	Multimodo 62.5 mm		Multimodo 50 mm		Unimodo
	Atenuación dB/km	Ancho de banda MHz-km	Atenuación dB/km	Ancho de banda MHz-km	Atenuación dB/km
850	3.2	160 a 200	3.0	400 a 600	-----
1300	1.9	200 a 600	1.2	400 a 1000	0.4 a 1.0

Tipo y diámetro de núcleo (µm)	Modos posibles	Longitud de onda (nm)	Distancia máxima (metros)	Ancho de banda máximo
Multimodo 50	300	850	1000	1 Gbps
Multimodo 50	300	850	300	10 Gbps
Multimodo 62.5	1100	850	275	1 Gbps
Multimodo 62.5	1100	850	33	10 Gbps

Elemento	LED	Láser semiconductor
Tasa de datos	Baja	Alta
Tipo de fibra	Multimodo	Multimodo o monomodo
Distancia	Corta	Larga
Tiempo de vida	Largo	Corto
Sensibilidad a la temperatura	Menor	Considerable
Costo	Bajo	Elevado

Monomodo
Sus medidas son 8.3 micras de núcleo y 125 micras de núcleo y cubierta

La luz viaja por el núcleo relativamente delgado del cable de modo único mediante un láser, sin reflejarse tanto en la cubierta como es el caso de la multimodo por lo tanto usa una única longitud de onda.

Tiene un diámetro pequeño, alrededor de 8 ó 9 micras, en el que se puede transmitir un solo haz de luz.

Multimodo
Sus medidas son 62.5 micras de núcleo y 125 micras de núcleo y cubierta

Puede soportar transmisiones simultaneas de varias ondas de luz.

Las distancias de transmisión no es tan grande como en las fibras monomodo debido a su bajo ancho de banda y la fuente de luz es más débil.

Se emplea en casos de enlaces cortos de 2 ó 3 Km., sin repetidores; redes locales de voz, vídeo y datos

Cableado estructurado

En el actual mercado ávido de información , la provisión de comunicaciones de voz y datos mediante un sistema de cableado estructurado universal, es un requisito básico que proporciona la base sobre la que se puede construir una estrategia general de los sistemas de información de una empresa.

Un sistema de cableado estructurado permite integrar todas las necesidades de conectividad de una organización. Está diseñado para usarse en cualquier cosa, en cualquier lugar y en cualquier momento. Además se instala una sola vez y puede adaptarse a cualquier aplicación (telefonía y redes locales) y migrar de manera transparente a nuevas topologías de red y tecnologías emergentes.

Los sistemas telefónicos y de informática se desarrollaron de manera separada.

Cada proveedor realizaba la instalación de cables que más le convenía, y este no podía ser usado por otros fabricantes.

Los equipos no eran compatibles con los diferentes tipos de cableado.

Cuando se deseaba agregar un nuevo cable había que quitar o rediseñar el cableado lo cual resultaba muy costoso.

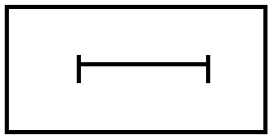
Era difícil el mantenimiento con frecuencia por no saber que cable estaba mal.

IV. ESTÁNDARES LAN/WAN

Estándares LAN

Estas tecnologías son implementadas de acuerdo a las necesidades de los usuarios de la red.Por esto se deben tener bien definidas las necesidades y los recursos con que se cuenta para hacer la mejor elección en la tecnología de red.

Ethernet
Estándar de transmisión de datos, para redes LAN.



Existen cuatro diferentes tramas de Ethernet:

802.3

Ethernet versión II

802.3 SNAP

Novell

La más común es el estándar 802.3. Algunos equipos activos, como los ruteadores, sólo reconocen los frames del tipo 802.3 y Novell, en tanto que los otros no son interpretados para las funciones de ruteo y similares.

Acceso al medio (CSMA/CD)

Es un estándar que se refiere a la forma de acceder al medio decidiendo quién transmite en la red.

- CS (Carrier Sense). Significa que antes de que una estación transmita en la red Ethernet, escucha si alguien esta ocupando el medio. Si es así espera un tiempo y vuelve a sensar, si el medio se encuentra desocupado, transmite.
  MA (Multiple Access). Significa que cuando una estación termina de transmitir, las demás tienen la misma oportunidad de transmitir su información.
  CD (Collision Detection). Se refiere a la habilidad de un adaptador Ethernet.

Características lógicas

- Colisiones: es el resultado de la transmisión simultánea en el medio.
- Existen dos diferentes tipos de colisiones:

A. Colisión temprana. Esta ocurre cuando no han transmitido más de 512 bits de la trama y se debe a que otras máquinas se encuentran hablando en el medio.

B. Colisión tardía. No es normal, ocurre porque el cableado esta en mal estado o no se cumplen con las especificaciones de los estándares (como cascadeo en más de cuatro niveles) y ocurre después de los 512 bits de la trama.

- Retardo de propagación: Es la relación entre la longitud máxima del cable y el tamaño mínimo de la trama.

Interrupción de trama

- Ruido eléctrico; causado por:
  - lámparas fluorescentes
  - máquinas de rayos X
  - cables de potencia, etc.
- Reflexión de la señal, causado por:

- Cables mal terminados
- Mala estructura de cableado

Estas interrupciones se dan, por lo general, al no cumplir con los estándares de cableado.

Colisiones causadas por:

a) no cumplir con especificaciones
b) hardware y cableado en mal estado
c) por desastres naturales

Codificación de la señal

- Código de línea: formato predeterminado para transmitir los dateos en señales de voltaje por el medio.
- Ethernet utiliza una codificación MANCHESTER
- Define como un bit 1 y 0 es representado eléctricamente.

Codificación Manchester

Codificación de la señal

Es utilizado en:

- -10 BASE-2. Es el estándar para la implantación de la red con cable coaxial delgado, la diferencia es la distancia de cobertura y el cable.
- -10 BASE-5. Es el estándar para la implantación de la red con cable coaxial grueso.
- -10 BASE-T. Es el estándar para la implantación de la red con cable de UTP.
- 10 BASE-FL. Es el estándar para la implantación de la red con cable de fibra óptica multimodo 62.5/125.

CARACTERÍSTICAS DE ETHERNET

Velocidad:	10 Mbps
Costo:	Relativamente barato
Estándar:	802.3
Protocolo de acceso al medio (MAC):	CSMA/CD
Topología de cableado:	Bus y estrella
Tipo de cableado:	Coaxial, UTP, F.O., AUI
Modo de flujo:	Half/Full duplex
Codificación:	Manchester

Fast ethernet

El nombre oficial es 100 BASE-T. Es parecido a la tecnología de Ethernet. Tiene una velocidad 10 veces mayor. Maneja mayor frecuencia en el medio. La codificación es diferente a la de Ethernet.
Incremento de información en la capa de enlace de datos
Es una extensión del estándar 802.3. Utiliza el protocolo MAC es CSMA/CD. La diferencia cae en la codificación de la señal en el medio. Mantiene una topología en estrella.

CABLEADO SEGÚN EL ESTÁNDAR

Tipo de salida	Cable	No. de pares	NOTAS
100 BASE T4	Categoría 3 UTP Categoría 4 UTP Categoría 5 UTP	4 4 4	100 metros de enlace
100 BASE TX	Categoría 5 UTP 150 ohms STP	2 2	Solo necesita de 2 pares para un enlace
100 BASE FX	62.5/125 um fibra multimodo	1	2 km. de enlace

El cuadro presentado muestra algunas características de las interfaces de Fast Ethernet y las características de cableado.

CARACTERÍSTICAS DE FAST ETHERNET

Velocidad:	100 Mbps
Costo:	Relativamente barato
Estándar:	802.3
Protocolo de acceso al medio(MAC):	CSMA/CD
Topología de cableado:	Estrella
Tipo de cableado:	STP, UTP, F.O., MII
Modo de flujo:	Full duplex
Codificación:	NRZI, MLT-3, 4B5B, 8B6T

Gigabit Ethernet

Este protocolo transmite a una velocidad superior a los anteriores, para ser precisos es de 1 Gbps. Es una extensión del estándar 802.3, puede desplazar a backbones de FDDI y compite con la tecnología ATM. Utiliza como protocolo de acceso CSMA/CD.

Emplea el mismo formato de trama Ethernet, así como el tamaño.

Tiene características adicionales como garantía de servicio, por ejemplo RSVP (Resource Reservation Protocol).

Propuesta de 1000 BASE-X

1000 BASE-LX. Implementado para transmisiones láser de longitudes de onda larga con enlaces arriba de 550 metros sobre fibra óptica multimodo y 3000 metros sobre fibra óptica monomodo.

1000 BASE-SX. implementado para transmisiones láser de longitudes de onda corta con enlaces arriba de 300 metros con fibra multimodo de 62.5 microns o 550 metros sobre cable de 50 microns multimodo.

1000 BASE-CX Diseñado para conectar dsipositivos de distancias cortas (por ejemplo en el mismo closet), este estándar puede ser usado con una distancia máxima de 25 metros.

1000 BASE-T. Este estándar permite la transmisión sobre cables categoría 5, 5e y 6 con una distancia máxima de 100 metros.

CARACTERÍSTICAS DE GIGABIT ETHERNET

Velocidad:	1000 mbps
Costo:	Depende de necesidades
Estándar:	802.3
Protocolo de acceso al medio (MAC):	CSMA/CD
Topología de cableado:	Estrella
Tipo de cableado:	UTP; F.O.
Modo de flujo:	Full duplex
Codificación:	8B/10

FDDI

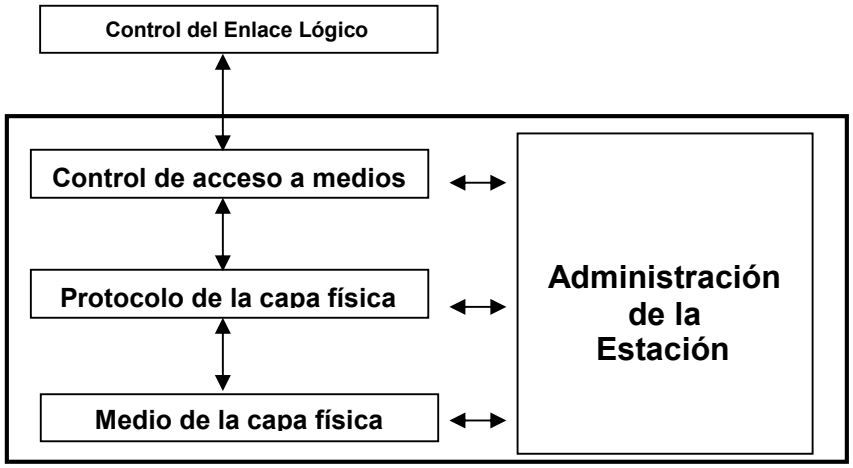
FDDI(Fiber Distributed Data Interface) es otro estándar de transmisión de datos para redes LAN. Específica una LAN con topología de anillo doble, a través del cual fluye el tráfico en direcciones opuestas (giro contrario). Tiene un método de acceso de estafeta circulante a 100 Mbps. Los anillos dobles consisten en uno principal y otro secundario. Existe la especificación en cobre CDDI.

Características FDDI:

- dos kilómetros de distancia máxima
- red basada en fibra óptica
- utiliza un código de datos 100 mbps
- topología de anillo
- baja tasa de error (una en un billón)
- conmutadores ópticos opcionales

tamaño de paquetes variable, máximo 4500 bytes
eficiencia de un 80% con una frecuencia de 125 Mhz

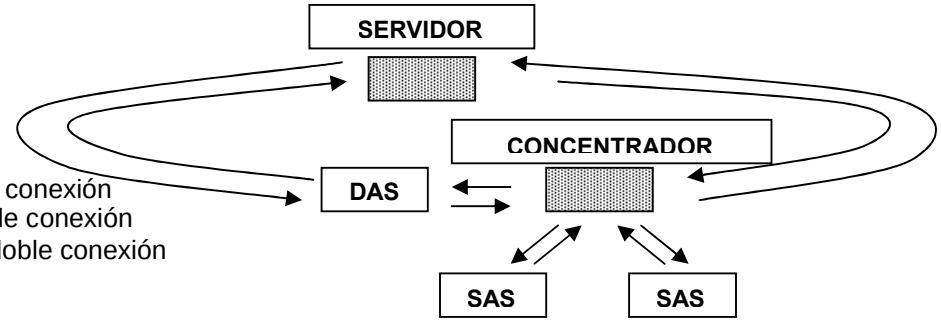
Especificaciones FDDI



MAC: Control de acceso al medio. Define como se accesa al medio de transmisión, formato de la trama, manejo de la estafeta, direccionamiento, algoritmos para el cálculo CRC y mecanismo de recuperación de errores.
PHY: Protocolo de la capa física. Define los procedimientos de codificación/decodificación, temporización, entramado.
PMD: Protocolo dependiente del medio físico. Define las características del medio de transmisión, enlaces, potencia, tasas de error, componentes ópticos y conectores.

SMT: Administración de las estaciones. Define la configuración de las estaciones de FDDI, configuración del anillo, inicialización, aislamiento, recuperación de fallas, estadísticas.

Tipos de conexión a las estaciones FDDI



SAS Estaciones de una conexión
DAS Estaciones de doble conexión
DAC Concentrador de doble conexión

Tolerancia a fallas FDDI
Anillo doble. Si una estación conectada al anillo doble llega a fallar o se apaga o si se daña el cable del anillo se envuelve automáticamente.

Interruptor óptico de desvió. Utiliza espejos ópticos para mantener la integridad del anillo, no se envuelve (en si mismo).

Dual Homing. Ofrecen redundancia adicional y garantizan la operación de la red, el dispositivo crucial se conecta a dos concentradores.

CARACTERÍSTICAS DE FDDI

Velocidad:	100 mbps
Costo:	Depende de necesidades
Estándar:	802.5
Protocolo de acceso al medio (MAC):	Token pasing
Topología de cableado:	Anillo doble
Tipo de cableado:	F.O.
Modo de flujo:	Full duplex
Codificación:	4B5B

Tipos de nodos en FDDI

1.Topología física de red:
- Anillo
- Estrella
- Malla

2.Configuración lógica:
Anillo doble

a) Acceso al doble anillo (Tipo A)
b) Acceso a un solo anillo (Tipo B)

Tipos de nodos
Un anillo principal es el que transporta los datos, el anillo secundario actúa como respaldo en caso de una falla en el anillo primario. Aplicaciones de FDDI: Backbone.

Aplicaciones de anillos de FDDI
Existen tres tipos de redes de computadoras en las cuales puede ser usada FDDI:

back-end

front-end

backbone

Back–end: Es la red usada para conectar un procesador con aparatos de almacenamiento, generalmente están localizadas en un solo local.
Front–end: Son usadas para conectar servidores o estaciones de trabajo, generalmente usadas en edificios abarcando uno o más pisos.
Backbone: Son redes usadas para conectar muchas redes, se utiliza entre campus.

Redundancia en el anillo de FDDI
Estación bypass: Aislan una estación y permiten la operación continua de anillo.

Anillo doble: Un cable de respaldo en espera para cada cable de red.

Anillo en forma de estrella: Todas las estaciones están conectadas a un concentrador pues hace más fácil el monitoreo y se aíslan fallas.

Estándares WAN

ISDN
ISDN (Red Digital de Servicios Integrados) se compone de los servicios de telefonía digital y transporte de datos que ofrecen las compañías regionales de larga distancia. El ISDN implica la digitalización de la red telefónica, que permite que voz, datos, texto, gráficas, música, vídeo y otros materiales fuente se transmitan a través de los cables telefónicos, con independencia de las fronteras geográficas, organizacionales y tecnológicas; es la convergencia de la informática y las telecomunicaciones. La evolución de ISDN representa un esfuerzo para estandarizar los servicios de suscriptor, interfaces de usuario/red y posibilidades de red y de interredes. Dentro de las

aplicaciones de ISDN están las de imágenes a alta velocidad, las líneas telefónicas adicionales en las casas para dar servicio a la industria de ventas por teléfono, la transferencia de archivos a alta velocidad y la videoconferencia. El servicio de voz es también una aplicación de ISDN.

Componentes de ISDN

Entre los componentes ISDN están las terminales, los Tas (Adaptadores de Terminal), los dispositivos de terminación de red, el equipo de terminación de línea y el equipo de terminación de central. Las terminales ISDN pueden ser de dos tipos. A las terminales ISDN especializadas se les conoce cono TE1 (Equipo Terminal Tipo 1).

A las terminales que no son ISDN, como los DTE que salieron antes que los estándares de ISDN, se les conoce como TE2 (Equipo Terminal Tipo 2). Los TE1 se conectan a la red ISDN a través de un enlace digital de par trenzado de cuatro alambres. Los TE2 se conectan a al red ISDN a trabes de un TA. El TA de ISDN puede ser un dispositivo individual o una tarjeta dentro del TE2. Si el TE2 se implementa como un dispositivo individual, se conecta al TA vía una interfase estándar de la capa física. Algunos ejemplos son la EIA/TIA-232-C, la V.24 y la V.35.

El siguiente punto de conexión más allá de los dispositivos TE1 y TE2 en la red ISDN es el dispositivo NT1 (Terminador de Red Tipo 1) o el dispositivo NT2 (Terminador de Red Tipo 2).

NT1 y NT2 son dispositivos de terminación de red que conectando el cableado de cuatro hilos del suscriptor con el ciclo local convencional de dos hilos. En Estados Unidos, el NT1, es un dispositivo del CPE (Equipo en las Instalaciones de Cliente). En la mayoría de los países, el NT1 es parte de la red que ofrece la compañía de larga distancia. El NT2 es un dispositivo más complicado que por lo general se encuentra en las PBXs (Centrales Privadas) digitales y que desempeña las funciones de los protocolos de las capas 2 y 3 y ofrece los servicios de concentración. Un dispositivo NT1/2 también puede ser un solo dispositivo que combina las funciones de un NT1 y un NT2.

La ISDN especifica una gran cantidad de puntos de referencia que definen las interfaces lógicas que conectan los agrupamientos funcionales, como los Tas y los NT1 Los puntos de referencia de ISDN incluyen lo siguiente:

R El punto de referencia entre el equipo que no es ISDN y un TA.

S El punto de referencia entre las terminales de usuario y el NT2.

T El punto de referencia entre los dispositivos NT1 y NT2.

U El punto de referencia entre los dispositivos NT1 y el equipo de terminación de línea en la red de larga distancia. El punto de interfase U tiene significado solamente en Estados Unidos, donde la compañía de larga distancia no ofrece la función NT1.

Servicios

El servicio BRI (Interfase a Tasa Básica) de ISDN presenta dos canales B y un canal D (2B + D). El servicio del canal B de BRI opera a 64 Kbps y su función es transportar datos de usuario; el servicio del canal D de BRI opera a 16 Kbps y su función es transportar información de control y de señalización, aunque puede soportar la transmisión de datos de usuario en determinadas circunstancias. El protocolo de señalización del canal D comprende de la Capa 1 a la Capa 3 del modelo de referencia OSI. La interfase BRI también ofrece el control de entramado, entre otras características, lo que permite que la tasa total sea de 192 Kbps. La especificación de la capa física de BRI es ls Y.430 de la ITU-T (Unión Internacional de Telecomunicaciones).

El servicio PRI (Interfase a Velocidad Primaria) de ISDN ofrece 23 canales B y un canal D en Estados Unidos y Japón, con una tasa total de 1.544 Mbps (el canal D de la interfase PRI opera a 64 Kbps). La interfase PRI de ISDN en Europa, Australia y otras partes del mundo ofrece 30 canales D más un canal D a 64 Kbps y una tasa total de la interfase de 2.048 Mbps. La especificación de la capa física de la interfase PRI está en la recomendación ITU-T Y.431.

Velocidades de ISDN

Canal A: 4 Khz (tradicional)

Canal B: 64 Kbps

Canal D: 16 o 64 Kbps

Canal H0: 384 Kbps

Canal H11: 1.536 Mbps

Canal H12: 1.92 Mbps

Tipos de servicio ISDN

Se clasifican de acuerdo con los grupos de canal que se forman como:

estructura de canal básico(BRI)

estructura de canal primario(PRI)

Protocolos de ISDN

Protocolo de múltple velocidad: Por la facilidad de combinar canales.

Protocolo de multimedia: Permite aplicaciones de voz, datos y video.

Protocolo de multipunto: Posibilita diferentes llamadas a la vez.

Tipos de conexiones en ISDN

Circuit switched sobre canales B

Conexiones semipermanentes sobre canales B.

Packet switched sobre canales B

Packet switched sobre canales D

Circuit-switched: este utiliza el canal B para datos de usuario y el canal D para señalización.

Conexión semipermanente: es una conexión determina por un período de tiempo establecido por el administrador.

Packet-switched: sobre canal B: la implementación de este servicio proporcionado por una red independiente.

Packet-switched: sobre un canal D: es el servicio habilitado desde la red ISDN.

ISDN maneja diversas aplicaciones que puede tener una red de datos, como es voz, datos, video, así como la señalización para la gestión del canal.

CARACTERÍSTICAS ISDN

Velocidad:	Canal A: 4 Khz (tradicional) Canal B: 64 Kbps Canal D: 16 o 64 Kbps Canal HO: 384 Kbps Canal H11: 1.536 Mbps Canal H12: 1.92 Mbps
Costo:	Depende de necesidades
Estándar:	Recomendación I del CCITT
Protocolo de acceso al medio (MAC):	LAPD
Topología de cableado:	Estrella, Malla
Tipo de cableado:	UTO, F.O.
Modo de flujo:	Full duplex

DSL

DSL (Digital Suscriptor Line) Son Líneas Digitales de Suscriptor, esta es la última innovación de las compañías telefónicas en líneas digitales. DLS es al menos tan rápido como una **T1**, pero a diferencia de ésta, DLS opera a través de cables telefónicos estándar de 2 hilos y ofrece servicios de alta velocidad a hogares y negocios.

T1 y T3 son líneas troncales que fingen como columna vertebral de las redes de conmutación de paquetes de larga distancia, ya que tienen gran ancho de banda. La velocidad de transmisión original (1.544 Mbps) es la línea T1, que se utiliza para interconectar WANS. El T3 tienen un ancho de banda de 44.736 Mbps y se utilizan comúnmente en WANS corporativas de gran tamaño y por los proveedores de servicios de Internet, y son extremadamente caras. Las T1 utilizan 4 hilos y ofrecen transmisión full-dúplex.

DSL utiliza la línea telefónica existente y en la mayoría de los casos no requiere de una línea telefónica adicional. Esto da un acceso a Internet continuo pero sin "amarrar" la línea telefónica. Con DSL no hay necesidad de que alguien cuelgue el teléfono, no hay señales ocupadas y no hay conexiones caídas.; además DSL ofrece un rango de velocidades de 144 Kbps a 1.5 Mbps (Esto es de 2.5 a 25 veces más rápido que un módem estándar de 56 kbps.

El servicio digital puede utilizarse para correr aplicaciones que requieren amplio ancho de banda, como audio/vídeo, juegos en línea, programas de aplicación, llamadas telefónicas, videoconferencia y otros. Además permite la separación entre el tráfico de voz y datos.

Configuraciones DSL

El servicio DSL está disponible en una gran gama de configuraciones:

ADSL: (Línea Digital Asimétrica de Suscriptor) Es la forma de DSL que se ha vuelto más familiar entre usuarios en hogares y pequeños negocios. Se llama asimétrica porque la mayor parte del ancho de banda dúplex está dedicado a la dirección de descarga, enviando datos al usuario. Solo una pequeña porción del ancho de banda está disponible para el envío o los mensajes iterativos del usuario. Generalmente se requiere para accesar a Internet debido a que el flujo de datos que entra por a la red opera mucho más rápido que el ruteo de datos fuera de ésta. Las velocidades de carga son más lentas que la de descarga. Esto no es de tanta utilidad para las WAN como lo es el acceso a Internet donde los datos que ingresan a la red son más importantes que los que salen. Utilizando ADSL se puede tener una velocidad de hasta 6.1 Mbits/s de descarga y 640 kbps de carga.

IDSL: (ISDN DSL) Este servicio monta una conexión DSL sobre una ISDN ya existente.

HDSL: (Líneas Digitales de Suscriptor de Alta Velocidad o High bit-rate DSL). Las HDSL transmiten datos a velocidades simétricas de las tasas de datos de T1 en E.U. o una E1 en Europa (2,320 Kbps)a través de distancias de 12,000 pies o menos. Las compañías telefónicas han utilizado las líneas HDSL para proveer líneas T1 por mucho tiempo, ya que se instalan mucho más rápido que las T1 y T3 convencionales.

SDSL: (Symmetric DSL).- En este las velocidades en ambos sentidos son iguales; es decir, la carga y descarga de datos se realiza a la misma velocidad. Es la misma cosa que HDSL con una línea individual, llevando 1.544 Mbps (E.U. y Canadá) ó 2.048 Mbps (Europa) en cada dirección de la línea dúplex.

RADSL: (DSL de Velocidad Adaptable) Son una herramienta común para las WAN´s que se encuentran más extendidas. Las RADSL son una tecnología de Westell que pueden modificar su velocidad como respuesta a las condiciones de la línea. Pueden operar a una distancia mayor de las centrales telefónicas que el resto de sus homólogos, pero existe la limitante a los 9 kilómetros. Sus velocidades varían de 640 Kbps a 2.2 Mbps en descarga y de 272 Kbps a 1.088 Mbps en carga.

VDSL: (Línea Digital de Suscriptor de Altísima Velocidad). Este servicio es el más rápido de la familia DSL. Estas líneas sólo tienen un alcance de 1,000 pies pero pueden operar a velocidades de una LAN (10 Mbps) o más rápido, por ejemplo de 51 55 Mbps en 1000 pies (300 mt) . Si se quisiera construir una WAN en un campus, la VDSL sería una buena alternativa y aunque es costosa, lo es menos que una T3 fraccional. Las compañías de estándares aún están trabajando en éste.

Otros servicios DSL son: CDSL, DSL Lite, UDSL y x2/DSL.
CDSL: (Consumer DSL) Es una tecnología DSL propiedad de Rockwell y es un poco más lento que ADSL.

DSL Lite: También se le conoce como ADSL sin "splitter" ó ADSL Universal. No requiere de splitter de la línea telefónica en la parte de usuario final, pero sí en la parte de la compañía telefónica. Se espera que este servicio de convierta en el tipo de DSL más comúnmente usado.

UDSL: (Unidireccional DSL) es una propuesta de una compañía Europea. Es una versión unidireccional de HDSL.

X2/DSL: Está planeado para módems de 3Com y de US Robotics que soportan comunicación a 56 Kbps con posibilidad de crecimiento y actualización a través de nuevo software.

Velocidades de DSL
Tabla comparativa de velocidades analógicas contra digitales utilizando DSL.

TIPO DE DATOS	TAMAÑO DE ARCHIVO	MODEM A 28.8 KBPS	DSL - 384 KBPS	DSL - 1.5 MBPS
Navegar en la red – 25 páginas Web con texto y gráficos.	2.5Mb	12 minutos	52 segundos	13 segundos
Un vídeo de 20 segundos	8Mb	37 minutos	2 ¾ minutos	43 segundos
Bajar la versión completa de Netscape 4.0 o Internet Explorer 4.0	25Mb	120 minutos	8 2/3 minutos	2 1/5 minutos

Hardware necesario
Un módem DSL o un ruteador con entrada para el módem DSL.
Tarjeta de Red NIC (Network Interface Card).
Splitter de teléfono para usar la línea telefónica convencional, si la compañía telefónica lo provee.
Línea telefónica convencional .

Beneficios de DSL
Servicio continuo.
Servicio de Internet y Teléfono simultáneamente.
Hasta 25 veces más rápido que el típico módem de marcado.
Buena relación costo-beneficio.
No hay señales ocupadas.
No hay caída de conexiones.
Descargas más rápidas.
Juegos más rápidos en línea.
Múltiples computadoras en una sola línea DSL.
Conexión dedicada y velocidad.
Operan con el mismo alambre de cobre que utilizan las líneas telefónicas convencionales.
El costo es más bajo que el de los servicios ISDN y T1.

Desventajas de DSL

Si la distancia máxima entre la oficina/residencia del cliente y la central telefónica es mayor a 9 kilómetros o 6 millas, no se puede utilizar el servicio. Este no es problema para WANS metropolitanas, pero sí para WAN´s suburbanas.

El módem DSL no permite conectar fax, así que para enviarlos o recibirlos tiene que utilizarse el servicio de fax de Internet.

No se encuentra disponible en todas las áreas.

Algunos tipos de aplicaciones no corren bien, como el video conferencia en dos sentidos y otras que requieren gran ancho de banda ya que el flujo de datos de estas aplicaciones está basado en paquetes.

No es apropiado para usuarios que requieren utilizar múltiples proveedores de servicio de Internet.

V. EQUIPOS ACTIVOS DE RED

Network Interface Card (NIC).
Interface para que un dispositivo se conecte a una red. También llamada “adaptador de red”. En equipos con procesador RISC, la interface de red está integrada al Mother Board generalmente.

Transceiver.
Transmisor-Receptor. Sirve para Adaptar Medios (de transmisión). Los estándares de red, principalmente Ethernet y FastEthernet, pueden utilizar varios medios de transmisión: par trenzado, cable coaxial delgado, grueso, fibra óptica, aire, etcétera.

Repetidor.
Este dispositivo sirve para extender una red: recibe y amplifica las señales. Trabaja en la capa física del modelo OSI. Sólo se pueden utilizar para extender redes bajo un mismo estándar de red. El número de repetidores que se puede usar para extender una red no es ilimitado, depende del fabricante tanto del repetidor como del resto de los dispositivos previamente conectados.
Una desventaja de los repetidores es que extienden el dominio de Broadcast de una red, ocasionando que el número de colisiones aumente así como también el tráfico.

Concentrador (Hub)
Proporciona servicio de conexión a uno o varios hosts mediante sus puertos. Existen concentradores para cada estándar de red (capa 1 del modelo OSI). La ventaja de este tipo de dispositivos es que aíslan los puertos que se encuentran dañados o sin conexión y permiten que el resto de sus conexiones continúen trabajando sin ningún problema.

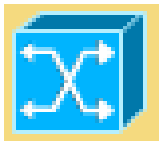
Puente (Bridge)
El puente, a diferencia del concentrador y el repetidor, trabaja en la capa de enlace de datos del modelo OSI. Hace las funciones del repetidor, pero además de extender la red, la segmenta.

Switch

El switch trabaja en la capa 2 del modelo OSI. Brinda conexión a hosts entre sí, asegurando el ancho de banda entre ellos mediante el establecimiento de conexiones virtuales.

Switch

Switch ATM



Ruteador

Sus funciones principales abarcan la capa de red del modelo OSI. Se encarga de enrutar los paquetes de datos por sus puertos de acuerdo a su tabla de ruteo. Los ruteadores son dispositivos imprescindibles para la interconexión de redes TCP/IP, AppleTalk, Novell IPX, etcétera.

Gateway

De acuerdo al modelo OSI, trabaja en la capa de aplicación. Su función, teóricamente, es hacer la conversión entre aplicaciones de arquitecturas diferentes.

Equipos híbridos

Son aquellos que cuentan con funciones específicas en diferentes capas del modelo OSI, generalmente en la capa 2 y capa 3.

Las WAN´s utilizan un gran número de tipos de dispositivos específicos para los ambientes WAN. Algunos de ellos son los switches WAN, servidores de acceso, módems, CSU/DSU y adaptadores de terminal ISDN a las WAN. Otros dispositivos para las implementaciones WAN son los ruteadores, switches ATM y multiplexores.

Switch WAN: Trabaja en la capa de enlace de datos.

Servidor de acceso: Actúa como concentrador para conexiones de marcación hacia adentro y hacia fuera.

Módem: Dispositivo que interpreta señales analógicas y digitales, permitiendo que se transfieran datos a través de líneas telefónicas de voz.

CSU/DSU: (Unidas de Servicio de Canal/Unidad de Servicio de Datos) Es un dispositivo de interfase digital que adapta la interfase física de un DTE a la del dispositivo DCE.

Adaptador de Terminal ISDN: Un adaptador ISDN (Red Digital de Servicios Integrados) es como un módem ISDN.

Puertas de enlace: Traductores de protocolos de redes similares. Se utilizan para enlazar LANS con WANS.

Ruteadores: Dispositivo que maneja el flujo de tráfico de paquetes cuyo destino no se encuentra dentro de la red local.

VI. PROTOCOLO TCP/IP

¿Qué es TCP/IP?

TCP/IP es un conjunto de protocolos de red que proporcionan comunicaciones a través de redes interconectadas de computadoras con diversas arquitecturas hardware y variados sistemas operativos. Por ser un sistema abierto, TCP/IP incluye estándares de cómo se han de comunicar las computadoras y reglas para conectar redes y encaminar el tráfico. Las siglas significan: Protocolo de Control de Transmisiones/Protocolo Internet y se deben a los dos protocolos más importantes los cuales quedaron definidos en 1982.
Son varias las asociaciones y organismos que intervienen en la regulación de TCP/IP, entre ellas podemos identificar a la ISOC, Internet Society como la más importante; ya que son los responsables de aprobar las tecnologías que aplican a su desarrollo. A su vez, esta es integrada por:

IAB, Internet Arqchitecture Board; le corresponde la aprobación de los RFC's
IANA, Internet Assigned Number Authority
IRFT, Internet Research Task Force
IETF, Internet Eingeener Task Force

RFC´s, Request for Comments

Son los documentos oficiales del IETF, que definen los estándares de TCP/IP. Su propósito es proporcionar un medio a un grupo diverso de usuarios de Internet para comunicarse y conciliarse dentro de la arquitectura y funcionalidad de Internet.
Hay mucho tipos de RFC's pero todos tienen la misma intención y algún aspecto similar en su formato, algunos son proyectos que ambicionan llegar a ser estándares, otros tienen naturaleza de tutorial o los hay bastante técnicos; pero todos los RFC son de hecho, el medio para que Internet pueda ser organizada y permitir a sus usuarios comunicarse. En general, se clasifican en cinco categorías; Requeridos, Recomendados, Electivos, Uso limitado y No recomendados.
Si alguno de estos documentos se puede considerar como un estándar, entonces sigue un proceso de desarrollo, prueba y aceptación, que igualmente contamos con tres niveles de maduración: Propuesta de Estándar, Borrador Estándar e Internet Estándar.
Cuando un RFC's es aprobado y publicado se le asigna un número, un documento nunca es actualizado, más bien es publicado en un nuevo RFC y se le asigna un número nuevo.
Encontramos una lista que hace referencia a los documentos que parece son los más importantes, todos ellos se pueden consultar por Internet y están al alcance de cualquier usuario que desee profundizar en la investigación.

RFC 791	Protocolo Internet (IP)
RFC 792	Protocolo de mensajes de control de Internet (ICMP)
RFC 793	Protocolo de control de transmisiones (TCP)
RFC 768	Protocolo de datagrama de usuario (UDP)
RFC 854	Protocolo de Telnet
RFC 959	Protocolo de transferencia de archivos (FTP)
RFC 821	Protocolo simple de transferencia de correo (SMTP)
RFC 822	Estándar para el formato de los mensajes de texto ARPA de Internet
RFC 1117	Números asignados
RFC 991	Protocolo oficial de ARPA en Internet
RFC 1034	DNS - conceptos y facilidades
RFC 1035	DNS - implementación y especificaciones

TCP/IP esta dividido en cuatro capas que definen el llamado Modelo DOD, cada una de éstas, se encarga de realizar una función o tarea especifica dentro de una red y también puede incluir diferentes protocolos. Figura no. 1.

Capas del Protocolo

Vamos a presentar una breve descripción de las capas y cómo es la comunicación entre ellas cuando se entrega o se recibe un paquete.

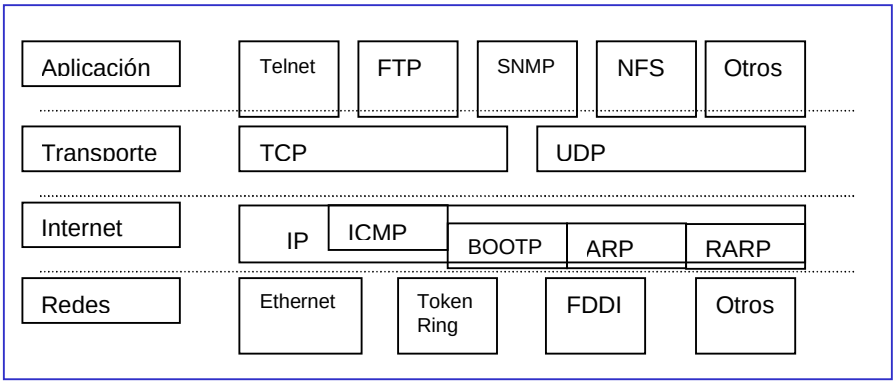


Figura no. 1. Descripción del modelo DOD y su referencia con TCP/IP

Capa Interfaz de Redes

Es la base del modelo y el nivel mas bajo. Esta capa es responsable de poner los frames dentro de los cables y fuera de ellos; es decir, es responsable de la transmisión de los datagramas sobre la capa física de la red y hasta el destino.

Cuando llega el paquete a esta capa, se agrega un CRC y un preamble; al recibirse en el host destino se descarga el preamble y se calcula el CRC si esta correcto la dirección MAC es examinada.

CRC: Cyclic Redundancy check, cálculo matemático que se añade para verificar que no ha sido corrupto el paquete.

Preamble: Secuencia de bits que identifican el inicio del paquete.

MTU, Unidad Máxima de Transferencia: Cada tipo de medio físico tiene un tamaño máximo de trama que no se puede superar, el nivel de redes o el nivel de enlace (modelo OSI) es el responsable de obtener esta unidad y de informar a los protocolos situados por encima.

Cuando se establece una conexión, los dos hosts involucrados intercambian sus valores MSS (tamaño de segmento máximo), y que para la conexión se utiliza el valor más pequeño de los dos MSS, el cálculo es él siguientes: MTU menos 40 bytes para los encabezados de IP y TCP.

Capa de Internet

Es el segundo nivel y es el responsable proveer la comunicación hots-to-host. Aquí es donde el paquete es encapsulado en un datagrama de Internet, los algoritmos de ruteo son cargados (ya sea estático o dinámico) y el datagrama es enviado a la capa de Redes para su transmisión. Los protocolos mas importantes son:

ARP: que es usado para obtener la dirección física de los hosts localizados en la misma red física.

ICMP: envía mensajes y reportes de error de los paquetes.

IP: es el principal responsable de la dirección y ruteo de los paquetes entre hosts y redes. IP para enviar un paquete le agrega su propio encabezado con las direcciones IP del host origen y del host destino, el protocolo que lo entrega, checksum y el TTL. Si el host esta en el mismo segmento de red lo envía directamente si no es el caso, el paquete es enviado al router.

Capa de Transporte

Provee la comunicación entre computadoras, El método deseado para la entrega de paquetes lo define el protocolo, de los cuales tenemos:

TCP que es orientado a conexión, establece comunicación para aplicaciones de transferencia larga y que requiere un mensaje de conocimiento de la información enviada.

UDP no es orientado a la comunicación por lo que no garantiza que los paquetes hayan sido entregados. Las aplicaciones que utilizan UDP son pequeñas y es su responsabilidad la entrega de los paquetes.

Son cuatro las características que hay que considerar cuando se habla de un protocolo orientado a conexión:

1. El camino para los paquetes se establece por adelantado
2. Los recursos necesarios para la conexión se establecen por adelantado.
3. Se asegura la reserva de los recursos durante toda la conexión
4. Cuando la transferencia de datos se ha completado, la conexión finaliza y se liberan los recursos.

Capa de Aplicaciones

Es la capa más alta, es donde las aplicaciones inician la cadena hacia el acceso por la red. Esta capa es la interfase con el usuario, contiene aplicaciones especificas. Entre las cuales tenemos: FTP, Telnet y SNMP, lo que son transferencias de Archivos y correos electrónicos, entre otras y varían de acuerdo al sistema operativo con el que estamos trabajando. Estas aplicaciones usualmente incluyen un cliente y un programa de servidores. A este programa se le refiere como daemon, que en la mitología griega significa “espíritu guardián”

La importancia de los números de puerto

Cada máquina en una red IP tiene al menos una dirección IP. Además, cada máquina tiene muchos procesos individuales en ejecución. Cada proceso puede llegar a ser un cliente de red, un servidor de red, o ambos. Obviamente, si el destino de un paquete se identifica sólo con la dirección IP, el sistema operativo no tiene forma de saber a qué proceso se envían los contenidos del paquete. Para resolver este problema, TCP/IP añade un componente identificado como puerto TCP o UDP. Cada conexión de una máquina a otra tiene un puerto de origen y un puerto destino. Cada puerto se etiqueta con un número entero del 0 al 65,535.

A fin de identificar cada conexión única posible entre dos máquinas, el sistema operativo tiene cuatro fuentes de información: la dirección IP origen, la dirección IP destino, el número e puerto origen y el número de puerto destino. La combinación de estos cuatro valores se garantiza que es única para todas las conexiones entre máquinas.

El modelo OSI

Los sistemas abiertos son sistemas diseñados para incorporar a cualquier dispositivo independientemente de su origen y aceptar también de otros fabricantes, para esto se generan los llamados estándares.

Los estándares se catalogan de dos maneras: estándares de facto y estándares de jure. Los estándares de jure los respalda un organismo como la ISO, ANSI, IEEE, etc. y como ejemplo tenemos: el código ASCII, POSIX, y el modelo OSI. Los estándares de facto existen porque cubren los huecos dejados por las especificaciones de los estándares de jure.

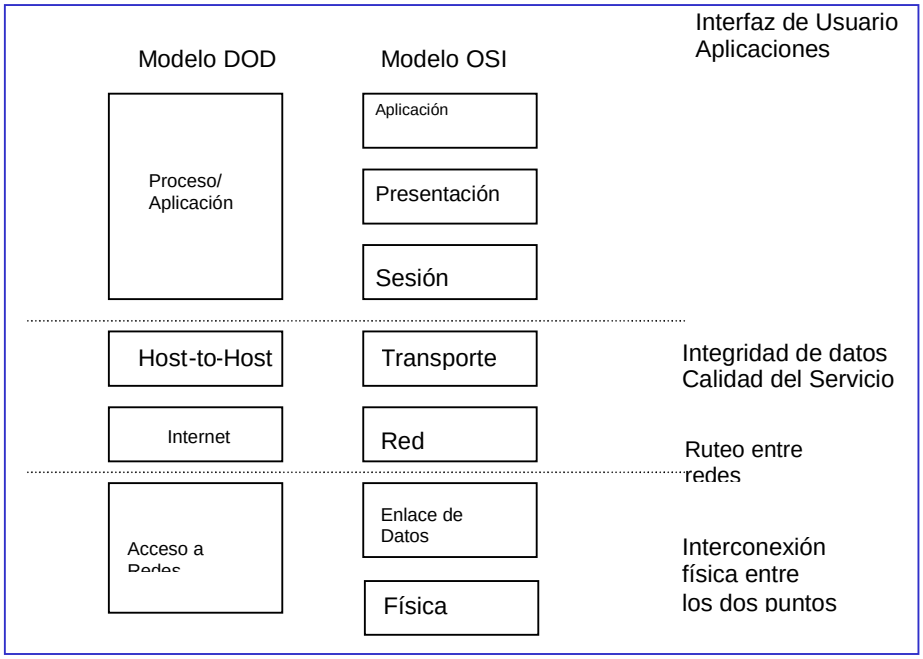


Figura no. 2. Cuadro comparativo entre el Modelo DOD y el Modelo OSI

Terminología TCP/IP y Protocolos

Llamamos paquete a la unidad de transmisión de tamaño máximo fijo que consta de información binaria que representa datos y una cabecera que contiene un número ID, direcciones origen y destino y datos de control de errores.

Un paquete de datos se mueve de una capa a otra dentro del stack de TCP/IP, cada protocolo agrega al paquete su propia información. El paquete con la información que se le va agregando recibe diferentes nombres técnicos como identificación a los protocolos. Estos nombres son:

Segmento: un segmento es la unidad de transmisión en TCP. Este contiene un encabezado y datos aplicación.

Mensaje: un mensaje es una unidad de transmisión de protocolos no-fiables como: ICMP, UDP, IGMP. Este contiene un encabezado del protocolo y datos aplicación o datos-protocolo.

Datagrama: es la unidad de transmisión IP. Contiene un encabezado IP acompañado de datos de la capa de transporte y también se considera como no fiable.

Frame: un frame es una unidad de transmisión en la capa de interfaz de redes y consiste de un encabezado agregado por la capa de interfaces de red acompañado de datos capa IP.

El propósito de toda la información que contienen estos encabezados es ayudar a la red a que dirija los paquetes desde la máquina origen a la máquina destino. Una vez de que llega a la máquina destino, permite a la máquina decidir si quiere aceptarlo. El encabezado IP especifica qué máquina debería recibirlo y el encabezado TCP especifica qué aplicación de la máquina destino tomará los datos.

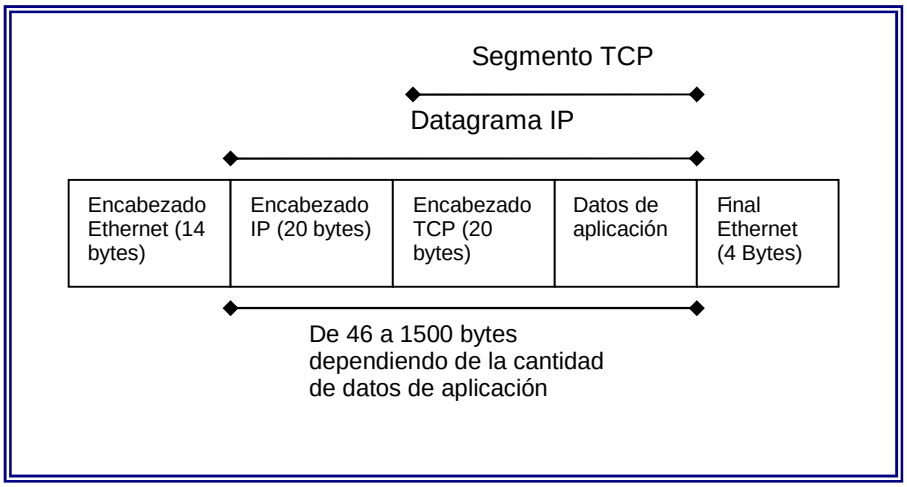


Figura no. 3. Un frame Ethernet con los encabezados de todos los componentes de un paquete TCP

Revisando los encabezados IP y TCP, vemos los campos que podemos usar para decidir si queremos aceptar un paquete. Los campos más interesantes son: Direcciones IP origen /destino y números de puertos origen / destino.
Los números de origen y destino son obvios (dónde va el paquete y de dónde viene). Comprobar contra qué números de puerto origen y destino se conecta nos permite elegir que servicios queremos permitir.

Componentes del Frame

Un frame que es el término para un paquete de datos en la capa de Interfaz de redes contiene tres componentes principales: el encabezado, datos y trailer.
Encabezado: incluye una señal de alerta para indicar que el paquete es transmitido, la dirección fuente y la dirección destino.

Datos: esta es la información actual enviada por la aplicación. Este componente varía en tamaño dependiendo de los límites configurados por la red. La sección de datos en la mayoría de las redes varia desde los .5 Kb hasta 4 Kb. En redes Ethernet el tamaño de los datos es aprox. 1.5 Kb.

Trailer: El contenido exacto varía dependiendo de la capa de interfaz de redes. Contiene un CRC (cyclical redundancy check) que es un número que se produce de un cálculo matemático en la fuente. Cuando el paquete llega al destino, el cálculo se hace de nuevo, si el resultado es el mismo indica que el paquete se ha mantenido estable.

ARP, Address Resolution Protocol

Para que los host de una red se puedan comunicar, es necesario que entre ellos se conozcan sus direcciones físicas, la resolución de direcciones es el proceso del mapeo entre las IP de los hosts y sus direcciones físicas.
ARP, es el responsable de esta función y lo hace a través del envió de broadcast a los hosts si están en una red local o al ruteador si es remoto. Una vez que se obtiene un mapeo se guarda una entrada en su caché, así, cada vez que requiere de una dirección primero checa si no la ha resuelto ya.

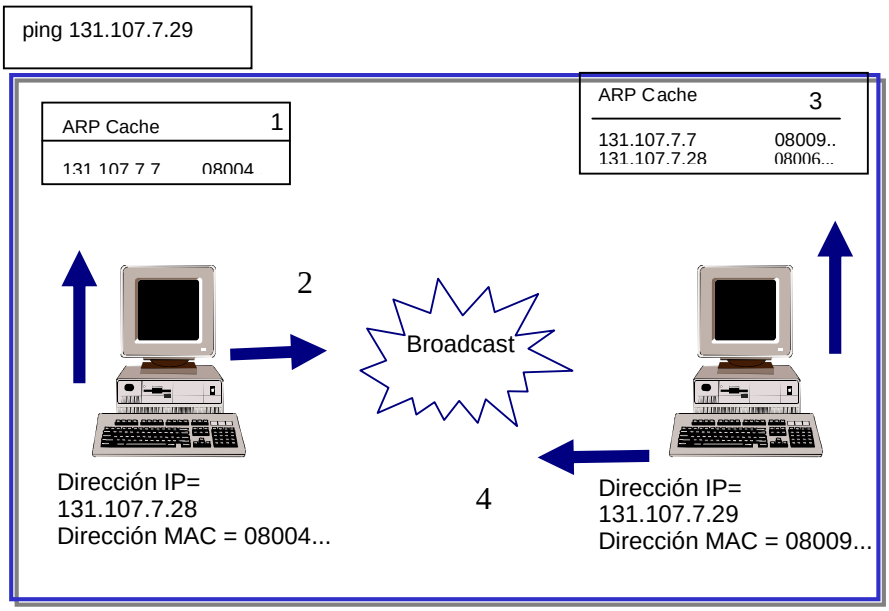


Figura no. 5. Proceso de resolución de direcciones en una red remota

ICMP, Internet Control Message Protocol

El protocolo de mensajes de control de Internet es un protocolo de mantenimiento especificado en el RCF 792. Los mensajes ICMP se encapsulan dentro de los datagramas de IP para que puedan encaminarse entre varias redes interconectadas. Se utiliza para:

Construir y mantener tablas de ruteo

A descubrir la Unidad de Transferencia (PMTU); se basa en los mensajes del destino no alcanzables RFC 1,191.

Diagnosticar problemas (Ping y Tracert)

Ajustar el control de flujo para prevenir la saturación de enlace de encaminadores

IP, Internet Protocol

Es el protocolo primeramente responsable del direccionamiento y ruteo de los paquetes entre los hosts. Protocolo de mensajería proporciona un sistema de envío de mínimo esfuerzo.
No esta orientado a la conexión, lo que quiere decir es que no establece una sesión antes del intercambio de datos. No garantiza la entrega de paquetes, Siempre hace su mejor esfuerzo pero por el camino puede ser extraviado, fuera de secuencia o duplicado.
Si IP identifica la dirección destino en una red local, transmite el paquete directamente al host. Si lo identifica en una red remota, entonces IP checa la tabla de ruteo para enviarlo al router que corresponde el host remoto.
Nota: Encontramos la definición de IP en el RFC 791.

Estructura del paquete IP

Campo	Función
Version	4 bits son usados para indicar la versión de IP
Header Length	4 bits para indicar él numero de 32 bits en el encabezado IP
Type of service	8 bits que son usados para indicar la calidad deseada del servicio por este datagrama en la entrega a través de los routers en la red
Total Length	13 bits usados para indicar el total de la longitud del datagrama
Identification	16 bits son usados como identificador para este específico paquete. Si el paquete es fragmentado, todos los fragmentos tienen el mismo numero de identificador
Fragmentation Flags	3 bits para las banderas del proceso o de fragmentación
Fragmentation Offset	13 bits para un contador que indica la posición del fragmento
TTL	8 bits para indicar el TTL o brincos antes de ser descargado
Protocol	8 bits para identificar el protocolo IP del cliente
Header Checksum	16 bits usados como checksum
Source Address	32 bits para almacenar la IP del host origen
Destination Address	32 bits para la dirección destino
Options and Padding	Un múltiple de 31 bits usado para almacenar las opciones de IP

TCP, Transmission Control Protocol

Es un protocolo de Internet orientado a conexión responsable de fragmentar los datos en paquetes que el protocolo IP envía a la red. Este protocolo proporciona un flujo de comunicación fiable y secuenciado para la comunicación de red.

El protocolo de control de Transmisión suministra a los programas un servicio orientado a conexión, fiable y de flujos de bytes. Los servicios de red se basan en el transporte TCP para iniciar la sesión, compartir archivos e impresión, duplicar la información entre controladores de dominio, transferencia de listas de examinadores y otras funciones comunes. Sólo puede utilizarse TCP para comunicaciones de uno a uno. TCP utiliza una suma de comprobación en ambas cabeceras y en los datos de cada segmento para reducir las probabilidades de corrupción que no se detecte en los datos.

Un mensaje de ACK (acknowledgment) es usado para verificar que los datos hayan sido recibidos por los otros hosts. Por cada segmento enviado, el host que recibe debe enviar un ACK.

Cuando no se recibe el mensaje de ACK, la información es retransmitida, igualmente, cuando un segmento es dañado se vuelve a enviar.

TCP Ports: Los ports de TCP proveen un especifico punto para entregar mensajes. Son alrededor de 256 port los que estas definidos como uso común. A continuación unos cuantos para referencia: FTP, 21; Telnet, 23; DNS, 53; NetBios, 139. TCP este definido en el RFC 793.

Estructura del paquete de TCP

Todos los paquetes de TCP tienen dos partes, una de datos y otra el encabezado. Los campos que contiene el encabezado son los siguientes:

Campo	Función
Source Port	Port del host que envía 16 bits
Destination Port	Port del host destino. 16 bits
Sequence Number	La secuencia en bits transmitidos por segmento. El número de secuencia es usado para verificar que todos los bytes fueron recibidos 32 bits
Acknowledgment Number	El número de secuencia de los bytes que host local espera recibir. 32 bits
Data Length	Longitud del encabezado 4 bits
Reserved	Reservado para uso futuro 6 bits
Flags	Este campo especifica el contenido del segmento
Windows	Que espacio esta disponible en la ventana TCP
Checksum	Verifica que el encabezado no este corrupto 16 bits
Urgent Pointer	Cuando un dato urgente es enviado (se especifica en el campo Flag). 16 bits

UDP, User Datagrama Protocol

El protocolo de datagramas de usuarios suministra un servicio no orientado a la conexión y no fiable. Se utiliza frecuentemente en comunicaciones de datagramas IP de difusión. Puesto que no esta garantizada la recepción de los datagramas UDP, los programas que lo utilizan deben elaborar sus propios mecanismos de fiabilidad.
UDP Ports: Para uso de UDP, la aplicación debe contar con la dirección IP y el número de puerto de la aplicación destino. Un port es la entrada por donde se reciben los mensajes. Por mencionar algunos ejemplos: Netstat,15; Domain, 53; TFTP,69; SNMP, 161.
Nota: El RFC 768 define el protocolo UDP.

¿Qué son las Direcciones IP?

Internet es un gran grupo de redes interconectadas. Todas estas redes se ponen de acuerdo para conectarse con otras redes, permitiendo a cualquiera conectarse a otro. Cada uno de estos componentes de red se asignan a una dirección de red.
Cada host en una red TCP/IP es identificada por una dirección IP. Cada uno de los componentes de una red TCP/IP debe tener una dirección IP para que se comuniquen entre ellos.
Las direcciones IP son una cadena de 32 bits que se dividen en octetos; los cuales están separados por puntos entre cada uno de ellos. Los octetos están representados por un número decimal que esta dentro del rango del 1 al 255, esto es a lo que se le llama notación decimal pero igual tenemos la notación binaria que es de donde parte este formato de direcciones. Ejemplo:

Formato Binario:	Formato Decimal:
10000011.01101011.00000011.00011000	131.107.3.24

Cada dirección define un número de red (Network ID) y un número de Hots (Host ID), el ID de la red es el número que identifica en el sistema que están localizadas en el mismo segmento físico de una red, por supuesto, todos los hosts en esta red tienen el mismo número de ID y que debe ser único en una Internetwork.
El host ID identifica la estación de trabajo, servidor, router o algún otro host de TCP/IP en un mismo segmento. La dirección para cada uno de los hosts debe ser única para el network ID.
Nota: un octeto son 8 bits, lo que en una notación decimal típica significa el primer conjunto de números. Por ejemplo: en la dirección IP 192.168.1.42 el primer octeto es el 192.

Convirtiendo direcciones IP

Recordando un poco, en el formato binario contamos nada más con dos valores: 0 / 1 que dependiendo de su posición dentro del octeto, cada número 1 tiene un valor decimal. Cuando tenemos un bit 0, su valor siempre es cero.
En la tabla que relatamos a continuación tenemos un ejemplo: todos los número 1 tienen un valor diferente siendo el mas alto el 128 y el mas bajo el 1. Para sacar el valor en notación decimal se requiere sumar la cantidad de cada uno de ellos, es decir: 1+2+4+8+16+32+64+128=255

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

Siguiendo lo anterior, tenemos la siguiente tabla:

Binario	Valores de los Bits	Notación Decimal
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

Clases de Redes

La comunidad de Internet decidió que las direcciones IP se dividieran en diferentes clases de redes, (A, B, C, D y E); de los cuales trabajamos con tres nada mas ya que los otros rangos están asignados a usos experimentales e investigaciones.
Para organizar mejor las clases de red, se decidió desde los primeros días de vida de IP, que los primeros bits deberían decidir la clase a la que pertenecían. Esto quiere decir que el primer octeto de la dirección IP especifica la clase.
TCP/IP soporta las clases A, B y C; las clases de redes se definen por el número de bits que son utilizados para identificar la red (Network ID) y los bits restantes son asignados a los dispositivos que componen la red. Igualmente define los posibles números de redes que hay dentro de cada clase y los números de hosts que puede haber por cada red.
Nota: Observará que algunos huecos en los rangos, esto se debe a que hay algunas direcciones especiales que se reservan para usos especiales. La primera dirección especial es una que ya le es familiar: 127.0.0.1. Está se conoce como la dirección de loopback o de bucle local. Se configura en cada máquina que usa IP para que se refiera a sí misma. Otros rangos importantes: cada IP de la red 10.0.0.0, de las redes 172.16 a 172.31 y de la red 192.168 se consideran como IP privadas. Estos rangos no se permiten reservar a nadie de Internet, y por tanto, puede usarlos para sus redes internas.

Definimos redes internas como redes que están detrás de un firewall, no conectadas realmente a Internet, o que tienen un enrutador que realiza el enlace de las redes.

Redes Clase A

Network	Host	Host	Host

En una red clase A, el primer octeto identifica la red y los tres octetos últimos el número de nodo.

El primer bit debe ser: 0xxxxxxx

Valor mínimo: 00000000 Decimal: 0
Valor máximo: 01111111 Decimal: 127
Rango: 1 –126

Hay 126 redes de clase A, cada una tiene 16,777,214 hosts.

Redes Clase B

Network	Network	Host	Host

En redes clase B, los dos primeros octetos son para identificar la red y los demás para el número de host.

Los primeros bits deben ser: 10xxxxxx

Valor mínimo: 10000000 Decimal: 128
Valor máximo: 10111111 Decimal: 191
Rango: 128 –191

Hay 16,384 redes de clase B, cada una tiene 65,534 hosts.

Redes Clase C

Network	Network	Network	Host

Los primeros bits deben ser: 110xxxxx

Valor mínimo: 11000000 Decimal: 192
Valor máximo: 11011111 Decimal: 223
Rango: 192 –223

Hay 2’097,152 redes de clase c y cada una tiene 254 hosts.

Redes Clase D

Las direcciones de las redes clase D están dentro del rango de 224.0.0.0 al 239.255.255.255 son usadas para paquetes multicast.

Los paquetes multicast usan muchos protocolos para alcanzar el grupo de hosts. IGMP Router Discovery es un ejemplo de un protocolo que utiliza paquetes multicast.

Redes Clase E

Igualmente, las direcciones de esta clase se encuentran dentro del rango del 240.0.0.0 al 255.255.255.255 y que están reservadas para futuros nodos de direcciones. Direcciones de las clases D y E no están asignadas a hosts individuales y más bien son para fines de investigación.

La siguiente tabla es un sumario de las diferentes clases de Redes y algunos valores a considerar.

Clase	Octetos	Inicia con Bits:	Número de Bits para identificar la red	Número de bits para identificar los host	Valor	Máscara de Red
A	NHHH	0xx	7	24	1 - 126	255.0.0.0
B	NNHH	10x	14	16	128 - 191	255.255.0.0
C	NNNH	110	21	8	192 - 223	255.255.255.0
D		1110	20	8	224 - 239	
E		1111	20	8	240 - 255	

Máscara de Red

Como mencionamos antes, las direcciones IP se dividen en dos partes, la dirección de red y la dirección de la máquina. Dependiendo de la clase de la dirección hay de 254 a 16 millones de direcciones disponibles para los hosts de la red.
Una máscara de red, es una dirección de 32 bits, que:
En primer lugar le dice al sistema que bits de la dirección IP corresponden al componente de red y qué bits corresponden al componente máquina.

Sirve para bloquear una porción de la dirección IP para distinguir él ID de la Red del número de los hosts.

Especificar cuando un host destino esta en una red local o remota.

Cada hosts en una red basada en TCP/IP requiere de una máscara, ya sea una máscara por defecto cuando la red no esta subdividida o una personalizada de acuerdo a los segmentos en que se haya dividido la red.

Volviendo un poco atrás, cuando en formato binario realizamos una operación AND tenemos que:

1	AND	1	=1
1	AND	0	=0
0	AND	1	=0
0	AND	0	=0

Este es el mismo proceso que TCP/IP utiliza para saber a donde debe enviar los paquetes que van de una red a otra, veamos. Si mi dirección IP es de una clase B, tenemos que:

Dirección Host	10011111	11100000	00000111	10000001
Máscara	11111111	11111111	00000000	00000000
Resultado:	10011111	11100000	00000000	00000000

Es de esta manera que la máscara bloquea la porción del Network ID para indicarnos de que clase de red estamos hablando. Las máscaras por default, las tenemos indicadas en una tabla anterior, para ser compatible con direcciones IP en notación binaria, la subnet mask también es convertida en binario.

Subnet Mask Bits

Representación Binaria	Representación decimal
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
11100000	224
11000000	192
10000000	128
00000000	0

En notación binaria, una máscara de subred es representada por cuatro octetos tal y como la dirección IP. La siguiente tabla le muestra las máscaras en notación decimal y binario utilizadas en el classfull método.

Representación DECIMAL	REPRESENTACIÓN binaria
255.0.0.0	111111111.00000000.00000000.00000000
255.255.0.0	11111111.11111111.00000000.00000000
255.255.255.0	11111111.11111111.11111111.00000000

Utilizando la representación en binario de la mascara usted puede manipular los 32 números. Esto incrementa la capacidad de proveer una mayor selección de redes comparado con el classful-method.

Subredes

Una Subnet o sub-red, es un segmento físico en un ambiente de TCP/IP que usa direccionamiento IP derivadas de una sola network ID.
Por lo general, las organizaciones adquieren su Network ID de parte del InterNIC, dividirla en segmentos requiere que cada segmento utilice un número diferente de network ID o digamos un Subnet ID. Este ID se crea dividiendo los bits que corresponden para identificar al host en dos partes, una parte se agrega a los bits que corresponden al ID de la red y la otra parte es para el ID de los hosts.
Para las organizaciones que aplican el subneteo, de una sola red crean múltiples segmentos; lo que les permite:
Mezclar diferentes tecnologías como: Ethernet y Token Ring

Reducir la congestión de la red, re-direccionando el tráfico y reduciendo los broadcast.

Una administración más cómoda de las direcciones IP

Conectar sucursales y tolerancia a fallas

Nota: El Subnetting, esta definido en el RFC´s: 950.

Implementando una Sub-red
Antes de crear un esquema de Sub redes, necesitamos determinar los requerimientos actuales y considerar el crecimiento de la organización.
Determinar el número de segmentos físicos que se requieren en la red

Determinar el número de hosts para cada segmento físico. Recordemos que cada uno de los hosts requieren una dirección IP.

En base a estas necesidades definir:

Una Máscara de Sub red para toda la red.

Un único ID para cada segmento físico
Un rango de hosts ID´s para cada sub-red

Cómo se crean las máscaras de subredes

Número de Sub-redes 0….. 254 Número de Hosts 254

Network ID			Host Id
10xxxxxx	Xxxxxxxx	**111**xxxxx	xxxxxxxx

Número de Hosts Posibles: 65,534

En la gráfica anterior, se ilustra como se toman bits extras de los asignados al host ID para formar una máscara de red. Por supuesto, podemos tomar más bits para más segmentos en el caso de necesitar más de 254; pero nos queda un número más pequeño de bits para combinar y crear los hosts ID. Por esta razón es muy importante una buena planeación.

Pasos para definir las nuevas subnet mask:

1. Determinar el número de segmentos que se requieren y convertir este número en binario.
2. Determinar el número de bits que nos tenemos que robar y comprobar
3. Convertir en decimal y definir la nueva subnet mask
4. Definir los segmentos de subred
5. Definir los rangos de direcciones IP para cada unode los segmentos

Ejemplo para una Red de Clase B:

1. Requerimos 6 segmentos convertidos en Binario tenemos: 0000110.
2. Lo cual quiere decir que ocupamos 3 bits que vamos a tomar del tercer octeto comprobando: 2 a la 3 es igual a 8, menos dos combinaciones que nos son posibles (ni todos ceros ni todod unos) es igual a 6 que cumple con los 6 segmentos que necesitamos.
3. La Sub-máscara en binario queda así: 11111111.11111111.11100000.00000000
4. Convirtiendo en decimal: 255. 255. 224. 0
5. Permutamos los bits que nos robamos para definir segmentos:
   a. Tercer octeto: 000xxxxx = 0 (no válido)
      a. 001xxxxx = 32
      b. 010xxxxx = 64
      c. 011xxxxx = 96
      d. 100xxxxx = 128
      e. 101xxxxx = 160
      f. 110xxxxx = 192
      g. 111xxxxx = 224 (no válido)
6. Definiendo los rangos de IP´s para cada segmento:

w.x.32.0	w.x.32.1 a la w.x.63.254
w.x.64.0	w.x.64.1 a la w.x.95.254
w.x.96.0	w.x.96.1 a la w.x.127.254
w.x.128.0	w.x.128.1 a la w.x.159.254
w.x.160.0	w.x.160.1 a la w.x.191.254
w.x.192.0	w.x.192.1 a la w.x.224.254

Cuando son pocos los bits que tenemos que combinar no representa un problema, pero que pasaría si son 7 ó 14?. Otro método que es un “shortcut” para la definición de los segmentos de red y de los rangos para las direcciones IP es:

1. Definir los bits que ocupamos para los segmentos, para este caso, requerimos 3.
2. Activar los bits en 1 de izquierda a derecha, esto es: 11100000
3. Seleccionamos el bit de menos valor, en este caso es el tercero y se convierte en decimal =32
4. Este es el valor que se debe incrementar para definir los segmentos, comparemos:

32 + 32 =64; 64+32 =96; 96+32=128; etc.

A continuación le relatamos una tabla de conversiones que le será bastante útil para planear su subnetting.

Clase A, considerar que se toma el segundo octeto para crear la máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.192.0.0	4,192.302
6	3	255.224.0.0	2,0972150
14	4	255.240.0.0	1,048,574
30	5	255.248.0.0	524,286
62	6	255.252.0.0	262,142
126	7	255.254.0.0	131,070
254	8	255.255.0.0	65,534

Clase B, en este caso es el tercer octeto que utilizamos para crear la máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.255.192.0	16,382
6	3	255.255.224.0	8,190
14	4	255.255.240.0	4,094
30	5	255.255.248.0	2,046
62	6	255.255.252.0	1,022
126	7	255.255.254.0	510
254	8	255.255.255.0	254

Clase C, recordar que es el cuarto octeto el que define la sub máscara

Segmentos	Bits requeridos	Máscara Sub-red	Hosts por segmento
0	1	Inválida	Inválida
2	2	255.255.255.192	62
6	3	255.255.255.224	30
14	4	255.255.255.240	14
30	5	255.255.255.248	6
62	6	255.255.255.252	2
126	7	Inválida	Inválida
254	8	Inválida	Inválida

Hasta ahora hemos subdividido redes en un solo- octeto, pero igualmente si las necesidades son más segmentos, una clase A se puede definir hasta el tercer octeto; por ejemplo:

Network ID	Subnet Mask	Binario
10.0.0.0	255.255.248.0	11111111.11111111.11111000.00000000

VII. SEGURIDAD EN REDES

Introducción

La seguridad tiene que ver con la protección de la información (activos) en cualquiera de sus estados:

- Creación
- Adquisición
- Almacenamiento
- Transmisión

Internet es un universo no acotado de computadoras multiusuario, heterogéneas e inseguras. Todas ellas intercomunicándose a través de dominios de seguridad que no comparten políticas o autoridad. Es una red de redes de alcance mundial, creada para facilitar la comunicación entre el gobierno y los investigadores. Actualmente millones de usuarios están conectados a Internet.

Internet proporciona infraestructura para la comunicación e intercambio de información, utiliza el protocolo TCP/IP para las comunicaciones, además de que se ofrecen servicios como:

- Correo electrónico
- Transferencia de archivos
- Acceso a sistemas remotos
- Conferencias interactivas
- Grupos de noticias
- Acceso a WWW

Problemas de Seguridad

Internet y TCP/IP no fueron diseñados pensando en seguridad, su filosofía es el proceso distribuido y comunicaciones abiertas. De este hecho se derivan sus principales vulnerabilidades

Facilidad para curiosear:

- El canal es promiscuo
- Los mensajes pueden ser interceptados por un tercero
- La mayoría del tráfico viaja en claro

Servicios de TCP/IP vulnerables
Complejidad en configuración de servicios
Código ejecutable: el código descargado de Internet y ejecutado localmente puede ser malicioso
Navegador inseguro: puede ser usado para robar información del sistema local

Existen otros factores que contribuyen a los problemas de seguridad como:
La facilidad de acceso a recursos: se puede acceder a Internet prácticamente desde cualquier lugar, actualmente existen más de 500 millones de usuarios, se estima que 2.5 millones son delincuentes.
Crecimiento acelerado: Las vulnerabilidades crecen con la complejidad de las infraestructuras internas, pues crece el número de puntos que pueden fallar, 2.3 millones de hosts se conectan a la red cada mes, no existen 2.3 millones de administradores de sistemas.
Falta de personal: Los encargados de los equipos pasan la mayor parte del tiempo resolviendo problemas, la aplicación de parches y medidas de seguridad se efectúa únicamente cuando sobra tiempo
Deficiente control de calidad en los productos de software: Por presiones del mercado se liberan productos que no se han aprobado adecuadamente, tienen problemas de seguridad

Existen algunos factores que dificultan la seguridad como:
El que la mayoría de administradores y responsables ignoran valor de sus activos, el temor de dañar la imagen pública, definiciones legales vagas o inexistentes, la persecución legal es difícil.

Las dificultades de la Seguridad se dan porque el delincuente debe rastrearse, no se cuenta con evidencias, es difícil asignar un valor a un dato, la mentalidad de “no dejar huella”, los delincuentes son vistos como intelectuales curiosos, los delincuentes computacionales no se ajustan a un estereotipo, las leyes y la ética frecuentemente son poco claras.

Otro aspecto es el ámbito de responsabilidad que rodea a cada uno de los problemas o incidentes, la mayoría de pérdidas o daños no son maliciosos (ignorancia de las políticas existentes, ignorancia del sistema), accidentes (cualquiera puede cometer un error), otro aspecto es conocer quién o quienes atacaron, cómo, con qué objetivos, si son personas (casi siempre es así) se necesita hacer clasificación de tipo y motivos, si son amateurs, si es por tentación por acceder archivos, si son empleados descontentos. Los Crackers y Hackers, si lo hacen por reto o curiosidad, los invasores corporativos, para obtener secretos corporativos, información interna o predicciones financieras.
La Inteligencia Externa como por ejemplo el Grupo de Alemania del Este (Cliff Stoll) o el Desert Shield / Desert Store, los terroristas que desean un control político, desestabilización, anarquía y caos.

Un sistema de Cómputo es un conjunto formado por hardware, software, datos, medios de almacenamiento, el personal involucrado, por lo que debe existir un compromiso con respecto a cualquier forma posible de pérdida o daño en un sistema de cómputo. *Comprometer* la seguridad de un sistema equivale a la posibilidad de provocar pérdida o daño al sistema, que puede explotarse intencional o accidentalmente. El punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

La amenaza es cualquier circunstancia potencial que explote una vulnerabilidad, para causar pérdida o daño al sistema como los ataques humanos, desastres naturales, errores humanos inadvertidos, fallas internas del hardware o del software, etc.

Tipos de Amenazas

Interrupción: cuando un activo del sistema se pierde, se hace no disponible o inutilizable, como la destrucción maliciosa de un dispositivo, el borrado de un programa o de un archivo de datos, malfuncionamiento del manejador de archivos del sistema operativo que tenga como consecuencia que no se pueda hallar cierto archivo en el disco duro .

Intercepción: cuando alguna entidad no autorizada logra acceso a un activo del sistema como el copiado ilícito de programas o archivos de datos, la intervención del canal para obtener datos sobre la red.

Modificación: cuando una entidad no autorizada logra acceso al activo del sistema y puede manipular ese activo. Como cambiar datos en una base de datos, alterar un programa para realice algún cálculo adicional o distinta a la que realiza, modificar datos en una comunicación, etc.

Fabricación: una entidad no autorizada puede fabricar objetos falsos en un sistema, como la inserción de transacciones espurias en un sistema de comunicación en red, agregar registros a una base datos ya existente.

Ataques y Tipos de Ataque

Un ataque es cualquier acción que explota una vulnerabilidad y los tipos de Ataques son:

Pasivos: Observa comportamientos o lee información, sin alterar ni el estado del sistema ni la información. Sólo afecta la confidencialidad del sistema o de la información. Ejemplos:

- Lectura o fisgoneo de mensajes

- Análisis de tráfico
- Siempre son antesala para un ataque activo

Activos: Modifica o afecta información o estado de sistema o ambos. Afecta no sólo la confidencialidad sino también la integridad y la autenticidad de la información o del sistema.

- Engaño
- Suplantación
- Réplica y modificación de mensajes
- Negación de servicio

Atacante es cualquier entidad que realiza un ataque. Puede ser una persona, un proceso, etc. Los nombres comunes para Atacantes son intruso, enemigo, “Cracker”, “Hacker”. Las suposiciones sobre el Atacante es que siempre está presente en un medio de comunicación público (como la red), sus objetivos son el obtener información en claro, la llave o ambos, acceder a los recursos del sistema, molestar, conoce los detalles del algoritmo y de la implementación. Se debe suponer que es capaz de interceptar, leer, alterar, modificar, cambiar, fabricar, retener, o reenviar información, interrumpir, desviar o retardar el flujo de información, engañar y suplantar a las partes legítimas en una comunicación, acceder a los recursos del sistema, molestar

Entonces, la seguridad no debe basarse en ocultar las herramientas de seguridad que se utilizan. Es decir, no debe usarse el clásico “*security by obscurity*” como premisa, sino l contrario, un buen algoritmo de seguridad debe ser público. La seguridad siempre debe residir en la fortaleza del algoritmo y en la llave, no en el hecho de mantenerlo oculto.

Algoritmo es una forma explícita de resolver un problema, puede ser una de tantas formas, o ser la única forma conocida o trasladada esa forma de solución a un programa de computadora, es lo que se conoce como “serie de pasos, finitos y ordenados.....”

Protocolo es una serie de pasos tendientes a resolver una tarea específica, es una forma de usar los algoritmos para implementar servicios de seguridad, como por ejemplo: construir el protocolo de autenticación de UNIX, aquí el protocolo es la serie de pasos (intercambios) y el algoritmo es el DES modificado

¿Qué debilidades tiene el protocolo?

Los passwords es una contraseña (Algo que se sabe), se establece hasta que el usuario lo introduce como palabra clave. Pero está sujeto a pérdida, revelación, a ataques.
Los ataques a passwords pueden ser ataque por fuerza bruta, intentar todas las posibles combinaciones con palabras cortas o con palabras comunes. El ataque del password-usuario se hace con nombres de familiares, fechas de nacimiento, etc.

Los archivos de passwords, en el cifrado convencional se puede proporcionar el password, descifrar el password almacenado en una tabla y comparar los passwords. En el cifrado unidireccional se puede proporcionar el password, cifrar password y comparar con el password cifrado.

Seguridad Informática

Misión de la Seguridad Informática es facilitar el cumplimiento de la misión y objetivos de la organización, mediante implementación de sistemas que consideren los riesgos tecnológicos relacionados con la organización, sus aliados y clientes. Cómo adquirir, almacenar, procesar y transmitir información, preservando:

Confidencialidad (que la información sólo la conozcan quienes tienen derecho a ello)
Integridad (que la información no sea alterada sin autorización)
Autenticidad (que la información provenga de fuentes autorizadas, es una forma de integridad)

Disponibilidad (que los usuarios legítimos puedan usar la información cuando lo requieran)

En general, la seguridad de un sistema tiene que ver con técnicas, procedimientos o medidas que reducen la vulnerabilidad del sistema. La seguridad tiene como objetivos principales lograr confidencialidad, integridad, autenticidad y garantizar disponibilidad de la información y de los recursos de cómputo. Estos objetivos pueden traslaparse o pueden ser mutuamente exclusivos. Por ejemplo, requerimientos fuertes de confidencialidad pueden restringir severamente la disponibilidad.

Confidencialidad es que la información no sea revelada a entidades no autorizadas, aplica a la información durante su almacenamiento, procesamiento, transmisión.
Integridad es un poco más difícil porque puede significar cosas distintas dependiendo del contexto como precisión, exactitud, inalterabilidad, modificación sólo en modos aceptables, modificación sólo por partes o procesos autorizados, consistencia, resultados significativos y correctos. Los aspectos de la Integridad, es común reconocer tres: las acciones autorizadas, la separación y protección de recursos, detección y corrección de errores.

La disponibilidad es similarmente compleja, se aplica a datos y recursos para uso aprobado. Algunos conceptos asociados son la presencia de datos y recursos en forma usable, la capacidad de responder a necesidades, respuesta en tiempo. Los objetivos de la disponibilidad de datos y de recursos son una respuesta puntual, asignación justa, tolerancia a fallas, utilidad o usabilidad, concurrencia controlada (soporte para acceso simultáneo, manejo de abrazos mortales, y acceso exclusivo cuando se requiera).
Control de acceso y relación con objetivos, en general, un control de acceso centralizado es fundamental para preservar confidencialidad e integridad, pero no es nada claro que un único punto de control de acceso sea capaz de garantizar disponibilidad. La mayoría de éxitos en seguridad se han logrado en áreas de confidencialidad e integridad, la protección para disponibilidad no ha sido posible lograrla por ahora.

Otros Objetivos de Seguridad son:
La asignación de responsabilidades (accountability) a nivel individual, es el requerimiento de que las acciones de una entidad puedan ser atribuidas a ésta de una forma única. Soporta directamente el no-repudio, aislamiento de fallas, detección de intrusos, recuperación después de la acción, acciones legales. El aseguramiento de que los otros cuatro objetivos han sido cubiertos adecuadamente, permite tener confianza en que las medidas de seguridad, técnicas y operativas: trabajan conforme a lo requerimientos de protección del sistema y la información que procesa.

Seguridad en Cómputo
Triángulo de Oro de la Seguridad en Cómputo:

- Confidencialidad
- Integridad
- Disponibilidad

Una definición más amplia incluye la seguridad física, seguridad en emisiones, seguridad personal.

Las preocupaciones de Seguridad, es ¿Qué características de seguridad pueden ser violadas y cómo?. Ejemplos:
Violaciones a Confidencialidad pueden hacerse a través de intervención y monitoreo de canales y líneas, obtención de información clasificada, obtención de información en general.
Violaciones a la Integridad son posibles por medio de alteración de registros de información, alteración de direcciones fuentes de correo.
Violaciones a la Disponibilidad pueden consistir en robo de tiempo de procesador (ciclos de reloj), negación de servicio (impedimento de usar los recursos y la información).

Servicios y Mecanismos

Para lograr objetivos de la seguridad, se establecen Servicios de Seguridad que se definen los objetivos específicos a ser implementados a través de Mecanismos de Seguridad que son los procedimientos o técnicas mediante los cuales se pretende proveer los servicios de seguridad.
En la arquitectura de seguridad OSI (Estándares ISO 7498-2 y ITU-T X.800) un *servicio de seguridad* es una característica que debe tener un sistema para satisfacer una política de seguridad, un *mecanismo de seguridad* es un procedimiento concreto utilizado para implementar el servicio de seguridad. En otras palabras, un servicio de seguridad identifica lo *que se quiere y un* mecanismo describe *cómo* lograrlo. La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

Confidencialidad
Autenticación
Integridad
Control de acceso
No repudio

La confidencialidad es garantizar que la información sólo pueda ser accesada por las partes autorizadas; por nadie más, es de los principales objetivos de la seguridad y es una herramienta para implementarla la criptografía

Autenticación, como proceso de identificación se clasifica en tres tipos, de acuerdo a la naturaleza de los elementos en que basa su implementación: En algo que se sabe, En algo que se tiene y En algo que se es.
También la autenticación puede ser directa o indirecta. La directa es en el proceso de autenticación solo intervienen las partes interesadas o que se van a autenticar, no interviene ninguna tercera parte actuando como juez. Y la indirecta es en el proceso interviene una tercera parte confiable que actúa como autoridad o juez, avala la identidad de las partes
La autenticación también puede ser unilateral, sólo una parte se autentica ante la otra. La otra parte no se autentica ante la primera. O Mutua donde ambas partes deben autenticarse entre sí.

El servicio de Autenticación está íntimamente relacionado al de Control de Acceso. Algunas de las principales técnicas de Autenticación e Identificación se revisarán el capítulo correspondiente a Control de Acceso.

La Integridad protege activos del sistema contra las modificaciones, alteraciones, borrado, inserción. En general, contra todo tipo de acción que atente contra la integridad.

No Repudio (NR), los Servicios de NR identificados por OSI son No repudio con prueba de origen, No repudio con prueba de entrega. No Repudio (NR) normal: para implementar NR se utilizan esquemas de llave pública como firmas digitales, pero no se restringe a ellas, también se pueden usar técnicas de cifrado de llave pública y de llave secreta, en esta última, siempre que se utilice una tercera parte confiable.

DoS y DDoS

Ataques y Herramientas

Ataques DoS Negación de servicios

Objetivo de todo ataque DoS:
Negar a algunos, o a todos los usuarios legítimos de un sistema o red, el acceso o utilización de un recurso o servicio en particular.

En los inicios de Internet (noviembre de 1988) surge el primer ataque DoS en Internet. El servicio se negó en dos formas:
Primera: múltiples copias de un gusano, limitaban la capacidad de procesamiento de los sistemas
Segunda: el temor de infectarse, mantuvo a Internet apagado por varios días

Un ataque DoS recorre uno u otro, o ambos, de los siguientes procesos: Negación de Servicio por Inanición del Recurso. Se debe, generalmente, a vulnerabilidades y configuraciones mal realizadas Negación de Servicio por Sobrecarga del Recurso. Esto se provoca cuando la demanda es mayor a la oferta.

La *disponibilidad* es el servicio más importante que DoS busca atacar. Comprometer disponibilidad de recursos compartidos puede generar una negación de servicios a través:

- Procesos
- Archivos compartidos
- Espacio en disco
- Porcentaje de uso de CPU

Principales entidades afectadas por ataques DoS:

- Usuarios
- Hosts
- Red

El intruso utiliza herramientas que explotan vulnerabilidades para acceder. Complementa el ataque usando algún método para destruir archivos, degradar procesos, degradar la capacidad de almacenamiento, causar la terminación de un proceso, apagar el sistema.

Los resultados, desde el punto de vista técnico, de un ataque DoS, son la corrupción de la información, mal utilización del recurso, indisponibilidad del servicio .

Estos resultados son el efecto, de los siguientes métodos:

- Destrucción o Modificación: de archivos del disco, o archivos individuales, tales como /etc/passwd ó etc/shadow
- Degradación de procesos: procesos múltiples (fork bombs), sobrecarga del CPU (procesos demandantes de CPU, gráficos, crackers de passwords por fuerza bruta, etc.), servicios de red. (inundación de peticiones a un servicio ó demonio, inundación de red por direcciones broadcast, ping de la muerte, etc.).

Degradación de almacenamiento

- Llenar la cuota o tamaño del disco que le corresponde al usuario, o llenar todo el disco
- Mail bombarder: genera archivos de gran tamaño, acabando con la cuota o el disco
- Mail spam: archivos prácticamente vacíos pero en número de miles, lo que acaba con los i-nodos

Terminación de Procesos
Ejemplo: uso de comandos como kill, bugs de software, o vulnerabilidades del software
Apagar el sistema
Ejemplo: el uso de comandos como shutdown , bugs de software, o vulnerabilidades del software

Modos de Ataque

Consumo de Recursos Finitos

- Memoria, espacio en disco, acceso a otras computadoras y redes, suministro eléctrico, ventilación. etc.
- Conectividad en Redes

Se refiere a cantidad de estructuras de info que cada servidor (servicio o demonio) es capaz de soportar. El atacante consume estas estructuras, que el kernel controla, impidiendo otras conexiones de usuarios legítimos
Ejemplo: conexiones “SYN flood“, el atacante crea conexiones incompletas (nunca devuelve el acknowledge para iniciar la sesión)

Utilización de Recursos Propios
Atacante usa recursos propios contra uno mismo
Ejemplo: paquetes UDP fraudulentos enviados al servicio *echo* de una máquina, para que los retransmita a la víctima al servicio *chargen*, estando estas máquinas en la misma red
Esto consume parte del ancho de banda de esa red y bloquea ambas máquinas, causando que se congestione y afecte a todo tráfico que pase por ella

Consumo del Ancho de Banda
- Consumir todo el ancho de banda disponible, generando paquetes grandes hacia una red dada
- Estos paquetes son del tipo IMCP ECHO, pero pueden ser de cualquier otro tipo
- El requisito es que sean de un tamaño no especificado o malformado (magic packets)
- Para éxito, el intruso debe coordinar varias máquinas, que funcionen como sus colaboradoras, en distintas redes. A esto también se le llama Ataque coordinado

Consumo de Otros Recursos
- Ejemplos: acaparar estructuras de datos con un script que cree copias de sí mismo
- Mail Bomber y Spaming
- Generar logs intencionalmente
- Colocar archivos en áreas de ftp anónimo o recursos compartidos
- Cualquier método que permita la escritura en disco
- Realizar intentos de conexión varias veces intencionalmente sin introducir el password correcto

Destrucción y Alteración de Información de Configuración
Un intruso destruye o modifica información de configuración (información para uso del sistema o para interconexión con la red). Ejemplo: la configuración del ruteador ó gateway de default, o el DNS. Si el sistema no presenta la configuración correcta, no mostrará interconexión

Destrucción o Alteración de los Componentes Físicos de Red
Importancia: seguridad física
Para evitarlo: Políticas de control de acceso a computadoras, ruteadores, closets de cableado, segmentos principales, fuentes de poder y UPS y, en general, todos los componentes críticos del cableado estructurado y de toda la red

Prevención y Respuesta a DoS

Directamente no existe forma práctica de evitar todos los posibles ataques DoS. Existe una serie de medidas que pueden evitar varios tipos de ellos. Implementar filtros en ruteadores para reducir el número de paquetes que utilizan el IP-spoofing. Tecnología actual del protocolo IP, hace imposible eliminar totalmente el IP-spoofing.

Reglas de filtrado: Si un paquete viene de fuera, no permitir el paso si la IP fuente es una dirección de la propia red interna. Si un paquete sale de la propia red interna, no permitir el paso si IP fuente es diferente de las direcciones de la propia red interna

- Deshabilitar cualquier servicio de red que no se use, o no sea necesario
- Habilitar sistemas de cuotas del s. o.

- Particionamientos adecuados para separar elementos críticos o esenciales (montar sistemas de archivos separados y con distintos atributos)
- Monitorear recursos y establecer rangos de actividad cotidiana o normal, para evaluar niveles de actividad inusual.Examinar recursos físicos, puntos de acceso (wireless), y cableado estructurado

- Usar herramientas de integridad (Tripwire) para detectar cambios en los archivos de configuración
- Invertir en "hot spares" (equipo que puede suplir rápidamente el servicio en el momento que suceda algo que bloquee el sistema principal)
- Establecer y mantener regularmente políticas de respaldos
- Establecer políticas de passwords para las cuentas privilegiadas

DDoS Negación de Servicio distribuido

DDoS es un procedimiento coordinado, ealizado por un conjunto de computadoras. El fin: generar inundación de paquetes, para sobrecargar una computadora, o una red completa.

Los ataques DDoS son una evolución de varios modos de ataques DoS, se consideran subclasificación de DoS. Muchas herramientas de ataques DDoS usan elementos de ataques de la clasificación DoS. Ejemplo (modo consumo de recursos finitos): las formas de ataques a conectividad, utilización de recursos propios, y consumo de ancho de banda, son parte medular de algunas de la herramientas más comunes de DDoS

Herramientas DDoS

No se clasifican como utilerías hackers. Son herramientas de penetración: no explotan ninguna vulnerabilidad de seguridad. Demuestran la cantidad de tráfico que un host o una red puede, o no puede, manejar. Muestran las debilidades de los protocolos de comunicación

Herramientas de Ataque DDoS

Concepto básico:
- Instalar gran cantidad de servidores de DoS en distintos hosts
- Estos hosts esperan comandos de un cliente, que indica a los servidores enviar tanto tráfico como les sea posible

Antes de ser parte de ataques DDoS, eran utilizadas por consultores de seguridad para hacer pruebas de consultoría de seguridad llamadas *Manejo de Capacidad.* Consiste en determinar cuánto tráfico puede soportar una red, mientras se prueba la confiabilidad de los servicios que ofrece

Antes, el consultor de pruebas de penetración realizaba telnet hacia todos los hosts que quisiera usar, conectarse como usuario y, manualmente, lanzar un comando que inundara un objetivo
En UNIX, el comando es ping -f *ipobjetivo*

Las herramientas actuales ya no solo hacen ping:
- Pueden enviar, por un nodo, miles de paquetes por minuto
- Por cientos de nodos, millones de paquetes
- Con miles de nodos, geográficamente dispersos, billones de paquetes por minuto

Con esta cantidad de paquetes, se puede bloquear cualquier cosa:
- ISP (proveedor de servicios de Internet)
- Granjas de servidores
- Ruteadores de banda ancha

Con estas herramientas se realizan distintas variantes, las cuales utilizan debilidades reales de los protocolos de comunicación

Herramientas de Ataque DdoS

TFN

- Contiene algunos bugs, funciones de control limitada
- Ataque de inundación por paquetes UDP (emulación trinoo)
- Ataque de inundación por TCP SYN (TCP SYN flood attack)
- Ataque de inundación de respuesta ECHO (ICMP Echo flood attack)
- Ataque Smurf
- Puede aleatoriamente seleccionar los 32 bits de la dirección fuente o solo los últimos 8 bits

TFN2K

- Realiza los mismos ataques que TFN, pero aleatoriamente y prácticamente al mismo tiempo
- Cifrado incluido para mejorar la seguridad de la red DDoS
- En el control de tráfico usa UDP/TCP/ICMP
- Las mismas funciones de falseo de la dirección fuente que TFN

Stacheldraht/StacheldrahtV4

- Contiene algunos bugs, funciones de control completas sobre la utilería
- Los mismos ataques básicos que TFN
- Las mismas funciones de falseo de la dirección fuente que TFN /TFN2K

shaft

- Pocos bugs, funciones de control completas sobre la utilería
- Añade estadísticas
- Ataque de inundación por paquetes UDP (UDP flood attack)
- Ataque de inundación por TCP SYN (TCP SYN flood attack)
- Ataque de inundación de paquetes por ICMP (ICMP flood attack)
- Realiza los tres ataques aleatoriamente

mstream

- Contiene muchos bugs, funciones de control muy limitadas
- Ataque de inundación por TCP ACK (TCP ACK flood (muy eficiente))
- Puede, aleatoriamente, seleccionar los 32 bits de la dirección fuente

Redes Virtuales Privadas

Principios de una VPN

Mecanismo que permite transmitir información sensible de manera segura a través de medios no confiables, utilizando técnicas criptográficas. Primeramente es necesario decir que una red privada es un enlace punto a punto que puede unir dos redes LAN. Este enlace privado no es accesado por personal no autorizado

Para lograr comunicación entre dos hosts o dos redes en distintos puntos geográficos: Necesario “tender” un cable que una dichas redes. El costo es sumamente elevado y el proceso de instalación muy lento. Con lo anterior se logra confidencialidad en los datos impidiendo el acceso no autorizado del exterior, pero ¿Qué hay con los usuarios internos?

Una red privada no es capaz de mantener la privacidad de los datos dentro de la organización. Puede proveer protección de los datos del exterior así como del interior de dicha red. No hay necesidad de “tender” un cable para unir las redes, reduciendo enormemente los costos y el tiempo

de configuración. La unión de dos hosts o dos redes LAN es a través de una red pública (ya tendida como Internet).

Los servicios de una VPN son:

- Autenticación
- Confidencialidad
- Integridad
- Control de Acceso

La implementación de una VPN es transparente para el usuario debido a los protocolos que la implementan

Los tipos de clasificación para una VPN son:

- Tipo de acceso que se tenga a la red VPN
- La implementación como tal de la VPN
- Comunicación que se establece entre las máquinas que soportan los protocolos para la VPN

Tipo de acceso de las redes VPN

- Intranet (site-to-site): Conectan ubicaciones fijas y utilizan normalmente conexiones dedicadas dentro de la estructura WAN de comunicaciones de la compañía
- Extranet: implantadas para ampliar los servicios de red y proporcionar un acceso limitado y seguro a los socios y clientes de la compañía, típicamente a través de Internet. Acceso remoto: Provee acceso seguro a usuarios móviles y pequeñas oficinas con necesidades muy básicas de comunicación

Comunicación entre las máquinas

- Host a Host: un cliente VPN se conecta a un servidor VPN y todo el tráfico se realiza entre el cliente y el servidor, lo cual significa que no existe el reenvío de paquetes hacia otra máquina
- Hots a Gateway: un host logra una comunicación con una red que se encuentra detrás de un gateway
- Gateway a Gateway: dos gateways que se comunican de forma segura los cuales reenvían la información a su red interna

De acuerdo a la instalación

- Sistemas VPN basados en Hardware: usualmente son sistemas basados en routers que cifran la información
- Sistemas VPN basados en Firewall: aprovechan los mecanismos de seguridad del firewall incluyendo el acceso restringido hacia la red interna
- Sistemas VPN basados en Software: Son ideales en situaciones donde ambos puntos de la VPN no son controlados por la misma organización y no requieren de altas velocidades

Diferentes Túneles

Existen protocolos que implementan un “tunel” cifrado y autenticado a través de Internet entre dos host, por ejemplo:

- SSH
- SSL/TLS

Los protocolos que trabajan en la capa 7 del modelo OSI, deben sustituir las aplicaciones actuales como telnet y ftp para SSH

En el caso de SSL/TLS se debe proveer el soporte para https

Protocolos VPN

Los protocolos que generan una VPN son:
- PPTP (Point-to-Point Tunneling Protocol)
- L2F (Layer 2 Forwarding)
- L2TP (Layer 2 Transport Protocol)
- IPsec (IP Security)

PPTP es un encapsulado PPP sobre IP
PPTP fue originalmente desarrollado por un consorcio que incluye Microsoft

Firewalls

¿Qué es un Firewall?

- Pared toda de fábrica, sin madera alguna, con el fin de que no se propague el fuego
- Vereda ancha que se deja en los bosques y sembradíos para que no se propaguen los incendios
- Punto centralizado de defensa entre dos o más redes

En Seguridad Informática un Firewall:

- Mecanismo para implementar las políticas de seguridad
- Simplifica la administración de seguridad de una o varias redes
- Ayuda a controlar el acceso de grupos de usuarios a servicios
- NO DEBE SER EL PUNTO ÚNICO DE FALLA

Un Firewall puede definir:

- Quién puede entrar
- Qué puede entrar
- Dónde y cómo pueden entrar

Tipos de Firewalls

Para Red: Firewalls de filtrado de paquetes, Firewalls de aplicación – Proxy, Híbridos
Para host: Firewalls personales, Norton Personal Firewall, Zone Alarm, entre otros.

Firewalls de filtrado de paquetes

- Basados principalmente en los encabezados de la capa de red y de transporte
- Actualmente, también permiten filtraje en base a interfaz
- Proporcionados por el sistema operativo
- Analizan paquetes de multiples protocolos
- Neutrales en cuanto a la aplicación
- Problemas para manejarlos con DHCP
- Normalmente transparentes

Firewalls de aplicación – Proxy
- Trabajan a nivel de la capa de aplicación
- Pueden ver el contenido del paquete
- Permite autenticación por usuario (vs IP)
- Son específicos a cada aplicación
- Originalmente usados solo para compartir servicios de Internet
- Actúan como un intermediario (Proxy)
- Pueden tener cache

Proxy

Proxy NO transparente: Hay que efectuar configuraciones especiales en los clientes
Proxy transparente: Menos complicados de instalar, El programa cliente no percibe su existencia

¿Cuándo usar un Firewall?

- Hay amenazas
- Existen vulnerabilidades
- Se cuenta con activos que proteger
- Se conoce contra qué o quién hay que defedenderse
- Se sabe que se pierde si no se protege
- Se tienen contramedidas a implementar con un Firewall
- Y el costo es menor que el beneficio

Identificar:
- Activos (Y su valor)
- Amenazas
- Vulnerabilidades
- Probabilidad
- Impacto

Decidir:
- ¿Cómo planeo la instalación de un firewall?
- ¿Qué procedimiento debo seguir?
- ¿Cómo se instala y configura?
- ¿Y después qué?

El esquema de distribución de grupos, servicios y Firewalls depende de cada organización.
- Bastion Host, filtros (Obsoleto)
- DualHomed, MultiHomed
- Red de servicios, TI, RH, DMZ, etc.
- FailSafe y Balanceo de carga Big/IP

Pasos para definir Esquema

Identificar:
- Grupos de personas
- Grupos de servicios
- Grupos de equipos (Hardware)
- Redes actuales

Agrupar personas, servicios y equipos en redes

Políticas para el Firewall

Definen los servicios de red que pasan por el Firewall y cómo
- Grupos de usuarios
- Quién los puede utilizar (origen)
- Para ir a dónde (destino)
- Cuándo se pueden utilizar (horario)
- Qué restricciones aplican (Filtros)
- Cómo los van a utilizar (Autentificación)

Pasos para definir Políticas
Identificar todos los grupos de personas
- Agrupar grupos de personas en redes (IP)
- Para cada red, identificar todos los servicios y destinos válidos
- Para cada servicio, identificar horario y reglas especiales (filtros, autenticación, NAT, etc.)

Características de las políticas
- Seguridad VS productividad
- Dos filosofías:
  Todo lo que no está permitido está prohibido
  Todo lo que no está prohibido está permitido
- Falla segura

Si se instala sobre una red en producción:
- Cerrar todos los servicios e irlos abriendo
- Abrir todos los servicios e irlos cerrando
- Instalar en ambiente de pruebas paralelo y migrar a producción

Componentes del Firewall
- Tipo de Hardware para Firewall
- Equipo dedicado:
- PIX, Nortel-fw1, otros
- Equipo de uso general:
- Intel
- Equipos Unix (SGI, SUN, HP, otros)

Otro tipo de Hardware a tomar en cuenta
- Los componentes dependen del cliente
- Tarjetas de red (Ethernet, ATM, DS0, etc.)
- Disco (IDE, SCSI, FibreChannel)
- CPU (Intel, SPARC u otros)
- Memoria RAM (> 64MB)
- CDROM (IDE o SCSI)
- Unidades de respaldo (ZIP, CD-R, etc.)

Coponentes del Firewall
- Software
- SO (Linux, Secure-BSD,IRIX, Win 2K, etc.)
- Refuerzos del SO (cerrar inetd, cops, tripwire, parches, logs, resp, etc.)
- Servicios básicos (Ruteo, NAT, DNS, DHCP, NetBIOS, etc.)
- Filtrado de paquetes (stateful, NAT, PAT)
- Proxies (CyberPatrol, Squid, HTTP, SMTP, SQL, FWTK, SNMP, RTSP, etc.)
- Otras apps (ISS, ssh, antivirus, cyberpatrol, activeX, java, swatch, arpwatch,reporteadores, VPN,etc)

Componentes externos al Firewall
- Usuarios
- Seguridad Física
- UPS (fallas eléctricas, sw de monitoreo)
- Cables y poder (120V,240V), ventilación
- Aplicaciones
- Protocolos de ruteo y otros
- Hubs, switches, ruteadores, cableado
- Balanceadores de carga
- IDS, otros Firewalls, etc.

Complejidad de Firewalls
Son muchos los elementos que hay que manejar en la implementación de un Firewall:
- Análisis de Riesgos, Políticas,
- Componentes, Esquemas, Distribuciones,
- Aplicaciones, etc.

No se suele poner suficiente atención a cada componente

Pasos para Instalar el Hardware
- Decidir qué hardware se va a comprar
- Revisar pólizas y políticas de instalación
- Revisar el diagrama de esquema de Firewall
- Seguir los pasos de instalación y recomendaciones del manual del equipo pedir al fabricante que realice la instalación y verificación del sitio
- DOCUMENTAR

Seleccionando el Hardware
La decisión depende de lo siguiente:
- Presupuesto
- Hardware disponible en el sitio y en el país
- Tipo de software de Firewall disponible para la plataforma
- Soporte sobre hardware y software
- Conocimientos del personal

Instalando el Software
- Identificar SO y versión a instalar
- Parches necesarios (Seguridad o funcionalidad)
- Particionar disco (Partición SO, swap, logs)
- Instalar SO mínimo (Lista mínima)
- Reconfigurar kernel (seguridad y rendimiento)
- Instalar y configurar software adicional (filtros netfilter, ipfilter, proxies, FWTK, Squid, aplicaciones)
- Reforzar SO (cops, tripwire, arpwatch, pam.)
- Respaldar

Configuración e inicialización del software
- Configurar redes y servicios básicos (IP, DNS, etc.)
- Configurar filtrado de paquetes
- Configurar proxies
- Correr tripwire
- Volver a respaldar todo el sistema
- Documentar la instalación y configuración(offline)

Puntos

- Los protocolos son bidireccionales
- En paquetes fragmentados
    - Sólo 1er fragmento contiene inf de capa transporte (puerto, bit ACK, etc)
    - Normalmente se dejan pasar el resto de los fragmentos (posibles problemas de seguridad)
- Necesitamos conocer características sobre los protocolos TCP y UDP

Características TCP

- Stateful (Estado de la conexión)
- Duplex (Ida y vuelta de paquetes)
- Orientado a conexión (ACK)
- Asegura llegada de paquetes (cuestionable)
- Es un protocolo más seguro que UDP
- Es propenso a ser filtrado

Características UDP

- Stateless (No lleva estado de la conexión)
- Simplex (Manda paquetes no regresan)
- No orientado a conexión
- No asegura llegada de paquetes
- Poco propenso a filtros
- Con stateful mejora la seguridad:
  Un paquete udp que sale sin que haya entrado petición correspondiente (Ej DNS)

BIBLIOGRAFÍA

1. **Ford, Merille**
   Tecnologías de Interconectividad de redes
   México
   Prentice May, 1998

2. **Cisco System, Inc**
   Academia de Networking de Cisco Systems, Guía del Primer año
   Segunda edición
   Madrid
   Person Educación, 2002

3. **Cisco System, Inc**
   Academia de Networking de Cisco Systems, Guía del Segundo año
   Segunda edición
   Madrid
   Person Educación, 2002

4. **Raya, José Luis**
   TCP/IP para Windows 2000 Server
   España
   Alfaomega Ra-Ma, 2001

5. **Press, Barry**
   Redes con ejemplos
   Buenos Aires
   Prentice May, 2000

6. **García, Jesús**
   Redes de Alta Velocidad
   España
   Alfaomega Ra-Ma, 1997

7. **García, Jesús**
   Redes para proceso distribuido
   España
   Alfaomega Ra-Ma, 1997

8. **Black, Uyless**
   Redes de Computadoras, Protocolos, Estándares e Interfaces.
   México
   Macrobit, 1992

9. **Stallings, Williams**
   Network Security Essentials: Application and Standards
   USA
   Prentice Hall, 2000