REDES

MEDIOS DE TRANSMISION

El tipo de medio que se utilice determina la velocidad de transmisión (expresada en número de bits por segundo bps o baudios) y la máxima distancia que puede existir entre los equipos que se intercomunican.

TÉCNICAS DE TRANSMISIÓN

Hay dos técnicas de transmisión de datos:

Banda Base

Usa señales digitales a través de una sola frecuencia. La señal fluye en forma de pulsos discretos de electricidad o de luz. Todo el canal se usa con la transmisión de una sola señal.

El ancho de banda es la diferencia entre la frecuencia más alta y la más baja soportadas por un cable. Algunos cables transmiten y reciben datos al mismo tiempo. A lo largo del cable de la red, el nivel de la señal decrece y se distorsiona, por seguridad, el sistema de banda base utiliza repetidores para que la señal llegue con la intensidad original.

Banda ancha

Usa señales análogas y un rango de frecuencia. La señal es continua, esta fluye en forma de onda electromagnética u óptica. La transmisión es unidireccional, si se dispone de suficiente ancho de banda se podrían hacer varias transmisiones al mismo tiempo. Usan amplificadores para regenerar la señal. Se necesita una ruta para transmitir y otra para recibir datos. Hay dos formas de hacer esto:

- Mid−split : Divide el canal en dos rangos de frecuencia, un canal es usado para transmitir y el otro para recibir.
- Dual−cable: Se utilizan dos cables diferentes, uno para transmitir y el otro para recibir información. Esta forma es mucho más cara que la Mid−split.

TIPOS DE CABLE

La red de área local necesita un cableado que enlace a sus estaciones de trabajo individuales con el servidor y otros periféricos. Si solo se dispusiera de un tipo de cableado la elección sería sencilla, pero hay varios tipos de cableado. Se va a examinar las ventajas y desventajas de cada tipo.

Cable de par no trenzado

Es el medio más sencillo para establecer comunicación. Cada conductor está aislado del otro; la señal de voltaje o corriente se aplica a uno de ellos y la referencia o tierra al otro. Es muy utilizado en telefonía, pero su aplicación en transmisión de datos está limitada a la conexión de equipos entre distancias no mayores a 50 metros, con velocidades inferiores a los 19.2 Kbps.

Esta clase de cable se utiliza sobre todo para conectar computadores a equipos cercanos como impresoras o módem. Por lo general, estas conexiones necesitan múltiples líneas, por lo tanto, se debe utilizar cable multipar o cable plano (ribbon). Cuando se utiliza cable multipar hay problemas con la integridad de la información a causa del acople de señal entre los distintos conductores. Además, por la estructura abierta de

cada par, es muy frecuente la captación de interferencia electromagnética. Como en el lado de la recepción se espera la señal que hay entre cada conductor y tierra, cualquier ruido extra, en un conductor, altera por completo la información que lleva.

Cable de par trenzado

Es el más barato de todos los tipos de medios de transmisión. Consiste en dos conductores aislados trenzados entre sí de modo que cada uno este expuesto a la misma cantidad de ruido de interferencia procedente del entorno que el otro. Al trenzar los hilos el ruido se reduce, pero no se elimina.

Los conductores tienen un número de calibre, para los usos en redes, los cables de calibres 22 y 24 son los más comunes. Entre más pequeño sea el diámetro del hilo, mayor será la resistencia para la propagación de la señal. Un hilo largo con una gran sección transversal (cross−sectional) incrementa la intensidad de la señal.

Hay 2 tipos de cables de par trenzado:

No blindado (UTP): Se usa en la especificación 10 BASET. Es el tipo de cable más usado en la red LAN. La máxima longitud de un segmento es 100mtrs (328 pies).

Hay 5 categorías de UTP:

- **Categoría 1** transmisión de voz pero no datos. (cable para la red telefónica)
- **Categoría 2** Para transmisión de datos. Su velocidad de transmisión es de 4mbps y tiene 4 pares trenzados
- **Categoría 3** Transmisión de datos hasta una velocidad de 10mbps. Tiene 4 pares con 3 trenzas por pie.
- **Categoría 4** Transmisión de datos a una velocidad de 16mbps tiene 4 pares trenzados.
- **Categoría 5** Transmisión de datos a una velocidad de 100mbps tiene 4 pares trenzados.

El cable UTP es susceptible al *crosstalk.*

Blindado (STP): Es menos susceptible a la interferencia puede transmitir datos a mayor distancia. Tiene una cubierta en cinta metálica que lo aísla.

Los conectores utilizados para este cable son del tipo de los enchufes telefónicos. Las redes ocasionalmente usan los conectores RJ−11, que pueden conectarse con 2 o 4 cables. Sin embargo, estos también se emplean para las instalaciones telefónicas y resulta inconvenientes en una red, ya que conectar una tarjeta de red en un enchufe telefónico puede dañar tanto a la tarjeta como al computador. Los conectores RJ−45 son versiones más grandes del mismo diseño y tienen 8 conexiones de cable.

También se utilizan los conectores tipo DB que se pueden encontrar en las conexiones de instrumentos seriales como las impresoras. Hay tres tipos de conectores DB, DB−9 con 9 pines, DB−15 con 15 pines y DB−25 con 25 pines.

Este cable es ideal para las redes de bajo nivel, se utiliza en topologías estrella, dado su carácter flexible. La distancia de la transmisión obtenida depende del calibre, la condición de la línea, el ambiente de operación y la velocidad de la transmisión.

Las principales limitaciones del cableado con par trenzado son su falta de velocidad y su limitado alcance. Puede manejar flujos de datos de aproximadamente 1 Mbps sobre distancias de algunos metros.

Se debe tener en cuenta que:

- La longitud máxima de cable UTP entre nodos y Hubs es de 100 metros.
- Las patas 1,2,3 y 6 del conector RJ−45 son conectadas de manera directa. Las patas 1 y 2 son transmisoras y las 3 y 6 son receptoras.
- Se pueden conectar hasta 12 Hubs a un Hub central.
- Sin el uso de puentes, el cable UTP puede acomodar un máximo de 1024 estaciones de trabajo.

Consideraciones.

Puede utilizarse cuando:

- Tiene restricciones de presupuesto para la LAN.
- Se quiere una instalación relativamente fácil con conexiones simples.
- No utilizar par trenzado si se quiere estar seguro de la integridad de los datos, de transmisiones a grandes velocidades y a grandes distancias.

IBM soporta para su red Token−Ring el cable telefónico de par trenzado y sin blindar tipo 3 pero de calibre 22 o 24 y con un mínimo de 2 vueltas por cada pie. Mínimo debe tener 4 pares y 2 pares de reserva para la Token Ring.

La red AT&T exige 2 pares de hilos trenzados de calibre 24 con blindaje, un par para la transmisión de datos y otro para la recepción.

Cable coaxial

Existe desde 1940. Es casi tan fácil de instalar como el par trenzado pero es más resistente a la interferencia y atenuación. Es relativamente económico, liviano, flexible, fácil de trabajar y es seguro. Está formado por un conductor de cobre rodeado de un aislante que generalmente es un tipo de plástico flexible llamado PVC. Los cables que pasen por los *plenum (*pequeños espacios entre techos, paredes y pisos falsos de los verdaderos) no pueden producir gases tóxicos, por esta razón deben tener materiales especiales, que son más costosos y menos flexibles que el PVC. La camisa exterior de cobre o aluminio actúa como conductor y también proporciona protección.

Este cable fácilmente soporta velocidades de hasta 10 Mbps y con conectores especiales es posible alcanzar frecuencias de señal de hasta 100 Mbps.

Hay dos clases de cable coaxial:

Coaxial delgado (Thinnet): Tiene un grosor de 0.25 pulgada. Es de la familia RG−58 (ojo tabla!!!!!!!!). Tiene 50 omhs de impedancia. Consiste en un conductor interno rodeado por un aislante dieléctrico, un blindaje de hoja de metal, un conductor tejido y una cubierta exterior protectora. Es flexible y fácil de trabajar. Va conectado directamente a la tarjeta de red. Transmite bien hasta 185 metros, luego sufre atenuaciones. A una red construida con cable delgado se le aplica la nomenclatura 10BASE2: 10Mbps, banda base, máxima longitud de 200mts.

Las reglas para la instalación y la configuración de segmentos de cable coaxial grueso son:

- La longitud máxima de segmento debe ser 185mts.
- Cada segmento de red debe tener una terminación de 50 ohm en cada extremo.
- No puede conectarse en serie más de 5 segmentos de red y solo 3 pueden estar ocupados.
- La cantidad máxima de nodos por segmento es de 30.
- La distancia mínima de cable entre adaptadores de red es de 0.5 mts.
- La cantidad máxima de nodos en una red es de 1024.

- La distancia máxima entre 2 nodos es de 1425 mts.

Coaxial grueso (Thicknet): Relativamente rígido, lo cual le impide hacer recorridos difíciles. Tiene 0.5 pulgadas de diámetro. El conductor central esta rodeado por un aislante dieléctrico al que, a su vez lo rodea un blindaje de hoja de metal que también esta cubierto por un conductor tejido. La parte externa del cable tiene una cubierta protectora. Es utilizado para conectar varias redes pequeñas en thinnet. A una red construida con cable grueso se utiliza la nomenclatura 10BASE5: 10Mbps, banda base, máxima longitud de 500 mts.

Las reglas para la instalación y la configuración de segmentos de cable coaxial grueso son:

- La longitud máxima de segmento de red es de 500mts.
- Cada segmento de red debe tener una terminación de 50 ohms en cada extremo.
- No puede conectarse en serie más de 5 segmentos de red y solo tres de estos pueden estar ocupados. (Tener nodos conectados a ellos).
- La cantidad máxima de transceivers por segmento es de 100.
- La cantidad máxima de nodos en una red es de 1024.
- Los transceivers no pueden instalarse a menos de 2.5mts.
- Los cables de bajada no pueden ser más largos de 50 mts.
- La distancia máxima entre dos estaciones cualquiera es de 3000 mts.

El BNC (Britsh Naval Conector) también llamado conector de bayoneta, es un conector utilizado para este tipo de cable, es soldado al final del cable. El BNCT une el cable a la tarjeta o es utilizado para lograr una conexión de 3 vías: 2 conexiones para proporcionar un flujo recto para la red y otro para la tarjeta adaptadora de red. Para realizar una extensión, se unen 2 cables por medio de un conector BNC y el terminador BNC cierra el final de un cable de bus.

El cable coaxial en banda base tiene un solo canal que transporta en cada momento un solo mensaje a una velocidad muy elevada. Su conductor portador va rodeado por una malla de cobre y el diámetro total del cable suele ser aproximadamente 9.5 mm. La información digital se transmite en serie de bit en bit ocupando el ancho de banda del cable. Dependiendo de la LAN, el cable coaxial en banda base pude manejar un régimen de datos de 10 Mbps.

A causa de la limitación de un canal único no es posible transmitir por cables de banda base señales integradas compuestas por voz, datos e incluso vídeo. Una ventaja es su facilidad de conexión y el hecho de que la conexión y desconexión de estaciones de trabajo no perturba el funcionamiento de la red. Aunque la distancia máxima recomendada para una LAN en banda base es aproximadamente 3 Km, si se hace uso intensivo de la red parece más realista una cifra aproximada a 500 mts. Las redes en banda base tienen una buena velocidad de datos.

Ethernet, con interfaces y protocolos de comunicaciones no propietaria, usa cable coaxial de banda base.

En una configuración de banda ancha de cable doble, el cable coaxial forma una especie de autovía de doble dirección, constituida por 2 bandas, cada una de las cuales contiene varios canales.

Consideraciones

- Puede transmitir voz, vídeo y datos.
- Se utilizan para transmisiones de larga distancia a menor costo.
- Su tecnología es familiar y ofrece seguridad de datos.
- En lugares húmedos se debe utilizar cables especiales, debido a que si la humedad penetra causará ruido y toda clase de problemas difíciles de solucionar.
- Si se tocan la malla y el núcleo habrá corto. El ruido de la malla afectará el flujo del cable de cobre y

se destruirán los datos.

Fibra óptica

La fibra óptica proporciona un método excepcionalmente atractivo para transmitir datos y señales de todo tipo con un mínimo de perdidas y libres de ruido. Actualmente los productos de fibra óptica (cables, conectores, transceivers, etc.), ocupan un lugar común en la arena de las telecomunicaciones, las redes de transmisión de datos, la televisión por cable, los sistemas de control, los equipos militares y otras aplicaciones. Además las cifras revelan que la fibra óptica es un mercado muy rentable.

Una sola fibra de vidrio, del espesor de un cabello humano, puede transportar mas información que varios miles de pares telefónicos o de cables coaxiales, con un mínimo de perdidas. Adicionalmente, los cables de fibra óptica son livianos, seguros, estéticos y resistentes, pueden transmitir anchos de banda de varios gigahertz sobre distancias de cientos de kilómetros sin necesidad de repetidoras, no pueden ser interceptados por métodos corrientes, son inmunes a la Interferencia Electromagnética (EMI), las radiaciones nucleares y a otras formas de interferencia, no generan calor ni campos magnéticos, pueden transportar señales entre dispositivos con tierras separadas o conectados a voltajes diferentes, no pueden ser cortocircuitados, no transportan corrientes letales, ahorran espacio, pueden viajar a líneas paralelas de distribución de potencia, entre otras.

El cable esta formado por vidrio puro estirado hasta formar fibras muy gruesas para constituir el núcleo, medio físico de transporte de la información que es convertida por un transmisor en energía luminosa modulada. Con el fin de evitar las perdidas de luz por radiación, el núcleo va rodeado por un recubrimiento (cladding), es decir, una capa de vidrio con un índice refractivo menor que el que constituye el núcleo, este también puede ser de plástico. El filamento de vidrio esta rodeado por un amortiguador, este a su vez por kevlar (un material sintético mas duro que el acero) para una protección mayor. La cubierta protectora exterior esta compuesta por PVC o poliuretano negro la cual tiene como función principal proporcionar protección mecánica a la fibra o fibras del cable.

Dependiendo de su configuración óptica puede ser de construcción holgada o de construcción ajustada. En un cable de construcción holgada, las fibras no están en contacto directo con la estructura de PVC del cable, sino suspendidas en un relleno de gel que las protege de la humedad y las aísla de las fuerzas axiales y transversales externas a las que el cable podría estar eventualmente sometido. Debido a su robustez, este tipo de cables se destina para exteriores y tendidos telefónicos de larga distancia. No obstante, la presencia del relleno de gel crea algunos inconvenientes de instalación y mantenimiento. En el cable de construcción ajustada, las fibras están directa y continuamente en contacto con la estructura del cable, aunque protegidas por una cubierta plástica o de Klevar y elementos de amortiguamiento que las protegen del riesgo de avería ocasionado por fuerzas axiales y transversales ejercidas sobre el cableado. Son más flexibles y livianos que los de construcción holgada, sustituyéndolos en muchos casos. Se utilizan principalmente para usos militares tácticos y aplicaciones de cortas distancias, incluyendo redes de área local (LAN) y enlaces punto a punto entre ciudades, edificios, fabricas, etc.

Para poder usar cable de fibra óptica los PC, las compuertas y otros instrumentos que se conecten directamente a la fibra deben ser compatibles con este sistema o conectarse a través de un instrumento llamado controlador de fibra de vidrio que convierte las señales eléctricas en pulsos de luz y viceversa.

La fibra óptica tiene un ancho de banda muy grande, es muy delgada y ligera de peso; no le afecta la interferencia electromagnética procedente de la maquinaria pesada, (que esto es muy importante cuando el cable se tiende a través del hueco del ascensor), los sobrevoltajes en la líneas o bien los originados por descargas eléctricas, y gozan de una excelente seguridad.

En una red de fibra óptica se emplea un láser o diodo luminiscente (Light Emitting Decode o LED) para

enviar una señal a lo largo del núcleo del cable. Frecuentemente se utilizan repetidores ópticos a lo largo del circuito para amplificar la señal, de manera que llegue a su destino con toda su intensidad. En el extremo de recepción del cable, el mensaje se convierte de nuevo en una señal digital o analógica por medio de un fotodiodo. Por el cable puede ir una sola señal (monomodo) o pueden ir varias (multimodo). Pueden ser de índice gradual en el cual el índice de refracción disminuye lentamente desde el centro de fibra hacia su porción exterior, o ser de salto de índice en el cual el índice de refracción varia bruscamente. La fibra monomodo tiene un ancho de banda muy grande pero el resumido diámetro de su núcleo hace que sus empalmes sean extremadamente difíciles. Por otra parte el monomodo exige el uso como fuente luminosa de un láser, mucho mas caro que un LED. Las fibras multimodo tienen un ancho de banda menor pero su empalme es mucho más fácil. Las frecuencias modulares de índice gradual son el medio de transmisión mas caro, pero son los que proporcionan la máxima velocidad y distancia de transmisión.

Las fibras multimodo para cableado de redes vienen en grupos que van desde 2 a 24 fibras, siendo la norma los grupos de 2 a 4 fibras. Cada fibra es unidireccional, puesto que se transmite un haz de luz en una sola dirección, la comunicación en dos sentidos exige que en el cable haya otra fibra para que la luz pueda viajar en dirección opuesta.

En el cable multimodo la señal se desvanece mas a través de una distancia dada que en un cable de monomodo. Este desvanecimiento es un fenómeno llamado atenuación.

La variedad mas nueva de cables de fibra óptica usa una fibra plástica más barata y fácil de manejar pero atenúa mas la señal que la fibra de vidrio.

El Instituto Nacional Americano de Estandarización (ANSI) estableció una norma para que el nivel dependiente del medio físico (PMD) del interface distribuido de datos de la fibra (FDDI) trabaje en conjunción con una transmisión de datos de 100Mbps.

Un sistema en fibra óptica se compone básicamente de un transmisor o fuente de luz, un receptor o detector, el cable de fibra óptica propiamente dicho, una o más estaciones repetidoras y los elementos de interconexión correspondientes (conectores, empalmes, acopladores, etc.) Una vez modulada por el transmisor, la información viaja a través de la fibra en forma de energía luminosa y es desmodulada en el receptor.

Ventajas: · Insensibilidad a al interferencia electromagnética, como ocurre cuando un alambre telefónico pierde parte de su señal a otro. · Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.

· Carencia de señales eléctricas en la fibra, por lo que no pueden dar sacudidas ni otros peligros. Son convenientes por lo tanto para trabajar en ambientes explosivos.

· Liviandad y reducido tamaño del cable capaz de llevar un gran número de señales.

· Sin puesta a tierra de señales, como ocurre con alambres de cobre que quedan en contacto con ambientes metálicos.

· Compatibilidad con la tecnología digital.

Desventajas : · El costo

· Fragilidad de las fibras

· Disponibilidad limitada de conectores. · Dificultad de reparar un cable de fibras roto en el campo.

Redes en fibra óptica:

FDDI (Interface de Datos Distribuidos para fibras) paso testigo en anillo.

S/NET Estrella activa para su conmutación.

FASNET Red de alto rendimiento. Utiliza dos buses lineales unidireccionales.

EXPRESSNET Es similar a FASNET pero en lugar de utilizar dos buses, esta emplea solamente un bus plegado

Consideraciones

- Se utiliza cuando necesita transmitir a grandes velocidades y a grandes distancias en un medio seguro.

No la use sí:

- tiene presupuesto bajo
- No tiene un experto para instalarla apropiadamente.

COMPONENTES DE RED

Hubs (concentradores)

Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella. Son dispositivos que se encuentran físicamente separados de cualquier nodo de la red, aunque algunos Hubs se enchufan aun puerto de expansión en un nodo de red.

El hub tiene varios puertos a los que se conecta el cable de otros nodos de red.

Pueden conectarse varios Hubs para permitir la conexión de nodos adicionales

La mayoría de los Hubs tienen un conector BNC además de los conectores normales Rj−45. El conector BNC permite que se enlacen Hubs por medio de un cable coaxial thin. Al disponer del conector BNC, no se tiene que desperdiciar un puerto RJ−45 en cada Hubs para la conexión con otro hub. Por el contrario, ese puerto puede conectarse a un nodo de red. Además los Hubs conectados con cable thin, también se pueden instalar nodos de red con adaptadores thin en el mismo segmento de cable.

Repeaters (repetidores)

Es un dispositivo que permite extender la longitud de la red, amplifica y retransmite la señal.

Los repetidores multipuertos permiten conectar más de dos segmentos de cable de red. Es importante no olvidar que aunque el repetidor multipuertos permite crear una topología física de estrella basada en varias topologías físicas de bus, el propósito principal de un repetidor es extender la longitud máxima permitida del cable de la red.

Bridge (puente)

Es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN. Los puentes revisan la dirección asociada con cada paquete de información. Luego si la dirección es correspondiente a un

nodo del segmento de red actual, no pasara el paquete a otro lado. La función del puente es transmitir la información enviada por un nodo de una red al destino pretendido en la otra red.

Opera en la capa de acceso al medio (capa 2)

Los puentes también se emplean para reducir la cantidad de trafico en un segmento de red. Mediante la división de un solo segmento de red en dos segmentos y conectándolos por medio de un puente se reduce el trafico general de la red. El puente mantendrá aislada la actividad de la red en cada segmento a menos de que el nodo de un segmento envíe información al nodo de otro segmento en cuyo caso el puente pasaría la información.

Pueden ser programados para que sepan que direcciones se encuentran de que lado del puente o pueden identificarlo simplemente observando los paquetes y viendo de donde vienen y a donde van.

Routers (Ruteadores)

Son similares a los puentes, solo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo NOS????. Con un NOS común el ruteador puede ejecutar funciones más avanzadas de las que podría permitir un puente, como conectar redes basadas en topologías lógicas completamente diferentes como ETHERNET Y TOKEN RING . También determinan la ruta mas eficiente para el envío de datos en casos de haber más de una ruta.

Son mucho mas complejos que los puentes. Entienden el protocolo de los paquetes y traducen entre protocolos distintos. Si se quisiera conectar una LAN ETHERNET que maneja un protocolo con otra LAN ETHERNET que maneja otro protocolo diferente, necesitara un ruteador.

También sirve para enviar paquetes a través de rutas distintas cuando se conectan varias redes. Esto significa que los Ruteadores pueden enviarse por la ruta mas rápida, más barata, la mas confiable etc. dependiendo del criterio que resulte mas importante.

Existen dos clases:

Los estáticos: difíciles de mantener, ya que el administrador de red tiene que proporcionarles información sobre como seleccionar rutas para los paquetes.

Los dinámicos: Mucho mas inteligentes que los estáticos. Observan todas sus interfaces y construyen tablas que identifican las rutas optimas. Si una ruta falla y hay una conexión alterna disponible, un ruteador dinámico puede asegurar que el sistema de interredes soporte las fallas.

Sin embargo un ruteador básico solo conecta redes cuyos protocolos pueda entender.

Un ruteador esta diseñado de manera que si no puede canalizar los paquetes actúa como puente.

Gateways (compuertas)

Permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Este tipo de compuertas también permiten que se compartan impresoras entre las dos redes.

Una vez que se pasa a funciones tales como encontrar datos en un registro, o archivo, es necesario construir toda clase de controles, verificaciones y protocolos para establecer, verificar, mantener y usar los servicios. Aquí es donde se hace necesario un método para traducir una manera de solicitar y usar servicios de otra.

Las compuertas cubren este papel de traducción. Se colocan entre dos sistemas y convierten las solicitudes del emisor a un formato que puede ser entendido por el receptor.

Transceiver

Este dispositivo permite conectarse a los cables coaxiales de la red, ya sea para implementar una nueva rama de la red o una simple derivación para un solo computador. Este aparato tiene un dispositivo tipo tornillo que penetra el interior del cable coaxial y hace contacto con el conductor central, sin necesidad de cortarlo; la parte exterior del tornillo hace contacto con el conductor exterior para garantizar de esta manera una buena conexión eléctrica. Normalmente estos dispositivos pueden tener un conector AUI para hacer conexión con un computador o con un hub, y uno tipo coaxial para conectarse al cable principal de red o simplemente generar otra rama de la misma.

El transceiver tiene internamente un circuito electrónico que le permite transmitir y recibir los datos a través del cable y proteger el cable principal contra fallas que se presenten en el computador o la rama que está derivada de él. El cable que va del transceiver al computador tiene 5 pares de cable trenzado: uno para alimentar los circuitos del transceiver, dos para enviar y recibir datos y los otros dos para realizar funciones de control. Este cable tiene en cada extremo un conector AUI.

Tarjeta adaptadora de red

El papel de una tarjeta adaptadora de red es actuar como interfaz física o de conexión entre el computador y el cable de red.

Funciones:

Preparar datos desde el computador para el cable de red. Antes de que los datos puedan ser enviados para la red, la tarjeta adapta la señal para que pueda viajar. El camino por el que viajan los datos en el computador es el bus. Los primeros buses de 8 bits fueron de IBM, IBM PC/AT usó bus de 16 bits, algunos computadores usan buses de 32 bits. En el bus los bits viajan en paralelo, mientras que en el cable de red viajan en serie.

La tarjeta adaptadora de red toma los datos que viajan en paralelo, los agrupa y envía en serie por el cable de red, traduce las señales digitales del computador en señales ópticas y eléctricas para que puedan viajar por el cable. El componente responsable de esto es el transceiver.

Direcciones de red. La tarjeta de red indica la localización o la dirección del resto de la red para distinguir todas las otras tarjetas.

Las direcciones en la red son determinadas por la IEEE. Cada tarjeta tiene una dirección única quemada.

En las tarjetas que utilizan DMA(Acceso Directo a Memoria) el computador asigna algo del espacio de la memoria para la tarjeta, solicita datos al computador, en el bus mueve datos de la memoria a la tarjeta, almacena en RAM mientras transmite o recibe cuando los datos viajan más rápido de lo que puede manejar.

Enviar y controlar datos. La tarjeta transmisora y la receptora se ponen de acuerdo antes de enviar los datos en:

- Tamaño máximo del grupo de datos a enviar.
- Cantidad de datos que se envían antes de la transmisión (Confirmación).
- Intervalo de tiempo entre cada trozo de datos enviado.
- Tiempo de espera antes que la confirmación sea enviada
- Cantidad de datos que cada tarjeta puede retener antes de un sobreflujo

- Velocidad de la transmisión

Las tarjetas necesitan igual velocidad para transmitir. Algunas tarjetas tienen circuitos que permiten que se ajusten a la velocidad de otras tarjetas más lentas. Cuando todos los detalles de la comunicación han sido determinados, las dos tarjetas comienzan a transmitir y recibir datos.

Controlar el flujo de datos entre los computadores y el sistema de cableado.

Recibir los datos entrantes del cable y traducir en bytes para que la CPU las pueda entender.

Contiene hardware y firmware programado que implementa el control lógico de enlace (Logical Link Control) y las funciones de control de acceso al medio (Media Access Control).

Los adaptadores de computadores para cables son conocidos como NICs ("Network Interface Cards"). Estos conectan el computador físicamente al tipo particular de cable que ha sido seleccionado, traducen entre señales bus de PCs locales de bajo poder y señales de medios de red de alto poder para larga distancia más fuertes, y corren programas en su ROM que formatean las señales enviadas por cable. Es importante notar que ciertos tipos de NICs pueden enviar y recibir datos mucho más rápidamente que otros: hay token ring NICs de 4 mbps y de 16 mbps., Ethernet NICs de 10 mbps. y de 100 mbps, NICs FDDI de 100 mbps, etc. Con las crecientes necesidades de rapidez en las redes locales, regionales y globales, la elección de NICs apropiados para servidores y clientes, es un elemento importante en el diseño de una red.

Hay muchos tipos de NICs de diferentes fabricantes para los sistemas de comunicación más populares como ARCnet, Ethernet y Token Ring. Casi cualquier PC equipado con una tarjeta cualquiera puede comunicarse con otro PC que tenga una tarjeta de un fabricante diferente. Para fibra óptica se restringe el uso de tarjetas a las de un solo fabricante.

Existen muchos parámetros y opciones diferentes que deben configurarse en los diferentes tipos de tarjetas. En las tarjetas más recientes la configuración puede realizarse totalmente por medio de software.

Configuración de opciones y montaje

Algunas tarjetas se pueden configurar por software o por **jumpers**

Interrupciones (IRQ. Interrupt Request). A través de IRQ los dispositivos hacen peticiones de servicios al microprocesador.

Las IRQ son construidas dentro del hardware interno del computador y tienen asignados diferentes niveles de prioridad que el microprocesador puede determinar.

Cuando la tarjeta adaptadora de red envía un requerimiento (Request) para el computador, este usa una interrupción (Interrupt) que es una señal eléctrica enviada a la CPU del computador. Cada mecanismo del computador puede usar diferentes IRQ. Esta se especifica cuando el componente es instalado. (Configurado)

Los recomendados para instalar la tarjeta son el IRQ 3 o IRQ 5

(Tabla Cuaderno OJO!!!!!!!!!!!!!!)

Puerto base I/O. El puerto base de entrada/salida especifica un canal por el que fluye la información entre el hardware del computador y la CPU. El puerto se le muestra a al CPU como una dirección.

Cada componente de hardware en un sistema debe tener un número diferente de puerto base I/O.

(Tabla Cuaderno OJO!!!!!!!!!!!!!!)

Dirección de memoria Base. Identifica una localización en la memoria RAM del computador. Esta localización es usada por la tarjeta adaptadora de red como un área de buffer para almacenar los **frames** de datos entrantes y salientes , esto es llamado algunas veces la dirección RAM de arranque.

Frecuentemente la dirección de memoria Base para la tarjeta de red es D8000. Es necesario asignar una dirección de memoria base que no la este usando otro dispositivo.

Compatibilidad de tarjetas adaptadoras

La tarjeta debe:

- Encajar en la estructura interna del computador
- Tener el correcto tipo de conector de cable.

Las topología anillo requieren tarjetas físicamente diferentes de las usadas por BUS y APPLE usa un tipo diferente de método de comunicación de red.

Arquitectura data bus

Hay cuatro tipos de arquitecturas de bus de datos:

- **ISA:** (Industry Standard Architecture) Usada en computadores IBM PC XT y AT Hay para slot de 8 y 16 bits. La de 8 bits se puede colocar en un slot de 16 bits, pero la de 16 no se puede colocar en una de 8 bits. Es el standard de Arquitectura COMPAQ
- **EISA:** (Extended Industry Standard Architecture) Es utilizada por AST, COMPAQ, EPSON, HEWLETT − PACKARD, NEC, OLIVETTI, TANDY WYSE, ZENITH. Es de 32 bits y es compatible con ISA y tiene características adicionales introducidas por IBM en su arquitectura microcanal.
- **MICROCHANEL:** Es eléctrica y físicamente incompatible con el bus ISA, trabaja con un bus de 16 bits o 32 bits. Puede ser manejada independientemente por múltiples procesos.
- **PCI:** (Peripherial Component Interconnect) Bus de 32 bits. Es plug and play, esto quiere decir que la configuración de la tarjeta no necesita interacción del usuario.

Cableado y conectores de red

La tarjeta adaptadora de red desarrollo tres importantes funciones en coordinación de actividades entre el computador y el cableado:

- Hace la conexión física con el cable.
- Genera las señales eléctricas que viajan por el cable.
- Sigue las reglas específicas para controlar el acceso al cable.

Es común que la tarjeta tenga dos conectores. Estos se seleccionan por medio de configuración con **Jumpers o Dip switches.**

Una conexión de red Thinnet usa un conector BNC, una conexión Thicknet usa un 15− pin (AUI), por cable UTP usa el conector RJ−45 que tiene 8 conductos. Algunas topologías propietarias de par trenzado usan RJ−11.

Desempeño de Red

Si una tarjeta es lenta los datos no pueden ir rápidamente, se puede agilizar el desplazamiento de los datos en la tarjeta con:

- **DMA:** (Direct Memory Acess) El computador mueve los datos directamente del buffer de la tarjeta a la memoria del computador, sin usar el microprocesador.
- **Adaptadores de memoria Compartida:** La tarjeta adaptadora tiene RAM que comparte con el computador. Este identifica la RAM como si realmente estuviera instalada en el computador.
- **Sistema de memoria Compartida:** El procesador de la tarjeta adaptadora de red selecciona una sección de la memoria de computador y la usa en el procesamiento de datos.
- **Bus Maestro:** Se encarga de llevar los datos directamente a la CPU. No interviene el procesador del computador. Lo ofrecen EISA y Micrichanel.
- **RAM Buffering:** Los datos son guardados mientras la tarjeta los puede procesar.
- **Onboard Microprocessor:** Con un procesador la tarjeta de red no necesita que el computador ayude en el procesamiento de datos.

Redes inalámbricas

Las redes inalámbricas no están totalmente libres de cables; se conocen como híbridos la redes que mezclan componentes inalámbricos y componentes de redes cableadas.

Estas pueden:

- **Proveer conexiones existentes temporalmente.**
- **Ayudan a proveer copias (backup) de una red existente.**
- **Proveen cierto grado de portabilidad**
- **Extiende la red más allá de los límites de las redes de cobre o de fibra óptica.**

Usos

Ya que su implementación es difícil se debe usar para:

- **Gente en constante movimiento como médicos.**
- **Áreas aisladas**
- **Departamentos con cambios en las características físicas frecuentemente.**
- **Estructuras como edificios históricos**

Tipos

Hay tres categorías:

- **LAN: Una red inalámbrica típica muestra y actúa igual que una red cableada excepto por el medio.**

    - **Puntos de acceso. El transceiver algunas veces es llamado punto de acceso(broad casts). Emite y recibe señales de los computadores que lo rodean y pasa datos entre la red inalámbrica y la red cableada.**

La red inalámbrica LAN usa pequeños transceiver montados en la pared, para conectarse a la red inalámbrica los tansceiver establecen contactos radiales con componentes portátiles.

    - **Técnicas de transmisión.** Las LANs inalámbricas usan cuatro técnicas para transmitir:

- **Infra rojo.** Operan usando los pulsos infrarrojos que envían datos entre componentes. Tiene que generar

señales fuertes para que no se interrumpan con la luz. Tiene un ancho de banda alto.

Hay cuatro tipos de red infrarroja:

- Red en línea de vista: Transmite únicamente cuando tiene una línea

clara entre el transmisor y el receptor.

− Red infrarroja dispersa: La transmisión rebota en paredes y techo hasta

llegar al receptor. Esta es efectiva en áreas de aproximadamente 100

pies.

− Red reflectiva: Los transceivers son situados cerca del computador

transmisor en dirección de una localización en común que redirecciona

la transmisión hacia el computador apropiado.

− Telepoint Optical: Proviene del servicio banda ancha. Es capaz de

manejar alta calidad de requerimientos multimedia que puedan

provenir de redes cableadas.

Con infrarrojo se dificultan las transmisiones en distancias mayores de 100 pies.

- **Láser.** Similar a infrarrojo en que requiere una línea directa de vista y cualquier persona o cosa que interrumpa el láser dañará la transmisión.
- **Narrow band.** Es similar a la transmisión de estación de radio. El usuario sintoniza la transmisión y la recepción en cierta frecuencia. No requiere línea de vista y tiene un rango de transmisión de 500 cuadras. Debido a que la señal es de alta frecuencia no traspasa muros de seguridad. Transmite a 4.8 Mbps.
- **Spread−Spectrum.** Transmite señales sobre rangos de frecuencia. Esto supera los problemas de banda estrecha. Las frecuencias disponibles son divididas en canales o saltos. Adapta tonos en un salto determinando Longitudes.

    - **Transmisión punto a punto.** Es la transmisión de datos de un computador a otro para comunicarse entre varios computadores y periféricos. Puede ser implementado en computadores individuales o computadores de una red con transmisión inalámbrica de datos.

Esta tecnología involucra transferencia inalámbricas serial de datos que:

− Usa enlace de radio punto a punto rápida y libre de error en transmisión de datos.

− La transmisión penetra paredes, techos y pisos.

− Soporta tasas de transmisión entre 1.2 y 38.4 Kbps máximo 200 pies o una tercera parte de milla en línea de transmisión sin obstáculos.

Transmite entre computadores o entre computador y periférico, como impresoras o lectores de códigos de barras.

- **LAN EXTENDIDA:** Algunos componentes inalámbricos son capaces de transmitir a distancias más amplias permitiendo conexión entre dos o más LAN.

    - **Conectividad multipunto inalámbrico.** El puente inalámbrico enlaza redes sin utilizar cables en una distancia de hasta 3 millas. AIRLAN/Bridge Plus usa Spread− Spectrum.

El costo de utilizar este componente está justificado porque elimina el gasto de líneas arrendadas.

    - **Puentes inalámbricos de largo alcance.** Utiliza tecnología Spread−Spectrum. Es compatible con redes Ethernet y Token Ring. Transmite a máximo 25 millas. Su costo se justifica con la eliminación de los enlaces T1 y los microondas.

- **COMPUTACIÓN MOVIL.** Requiere de un teléfono portátil y una red de servicio público que transmita y reciba la señal. Puede ser:

    - **Comunicación Packet−Radio.** El sistema rompe la transmisión en paquetes. Incluye:

− Dirección fuente

− Dirección destino

− Información de corrección de errores.

Los paquetes son enlazados a un satélite que los emite. Unicamente los componentes con la dirección correcta los recibe.

    - **Red Celular.** (CDPD. Cellular Digital Packet Data) Utiliza la red análoga existente de voz para transmitir datos entre llamadas (voz) cuando el sistema no está ocupado, Es rápida pero se ve afectado por un retardo secundario que lo hace ligeramente más lenta que la transmisión en tiempo real.

    - **Estación de Satélite.** Las microondas son un buen método de comunicación en áreas pequeñas. Es una excelente forma de comunicación en :

− Satélites por enlaces terrestres.

− Comunicación entre edificios.

− A través de largas y planas áreas abiertas como cuerpos de agua o

desiertos.

Un sistema microondas consiste de:

− Dos radio Transceiver, uno para enviar y otro para recibir.

− Dos antenas direccionales que captan la señal de los transceiver. Son

instaladas en torres para levantar la señal sobre obstáculos que la

bloqueen.

Los estándares inalámbricos como el de las LANs inalámbricas 802.11, el de DECT, y el de Hiperlan fijan

unas bases necesarias para los servicios que trabajen en este ámbito. Las ventajas que proporciona el estándar 802.11 son la flexibilidad de los equipos, la robustez y el ahorro del cableado, pero tiene el inconveniente de la baja velocidad en que puede trabajar. Este inconveniente es solucionado en Hiperlan, ya que las características propias del sistema posibilitan velocidades de 20 Mbps.

****

TRANSMISIÓN DE INFORMACIÓN EN LA RED

Para garantizar que los computadores conectados en la red puedan comunicarse sin problemas, deben cumplir una serie de normas que se conocen generalmente con el nombre de protocolo.

TECNOLOGIAS CLASICAS

REDES ETHERNET

En 1973, Robert Metcalfe escribió una tesis para obtener el grado de PhD en el Instituto Tecnológico de Massachusets − USA en la que escribió la investigación que realizó acerca de las LAN. Posteriormente se trasladó a la compañía Xerox, donde formó un equipo de trabajo para desarrollar la red ETHERNET, basada en las ideas contenidas en su tesis.

Las redes ETHERNET pertenecen a la categoría de redes LAN, por eso es muy frecuente encontrarlas en oficinas, fábricas, entidades oficiales, universidades etc.

La ETHERNET desarrollada por Xerox tuvo tanto éxito que las compañías Xerox, DEC (Digital Equipment Corporation) e Intel propusieron a la IEEE una norma para la ETHERNET de 10 mbps. Esta norma fue la base para la hoy conocida IEEE 802.3,que aunque difiere un poco de su especificación inicial, conserva muchas características originales.

Este sistema se llamó ETHERNET, en honor al éter luminífero, a través del cual se pensó alguna vez que se propagaban las ondas electromagnéticas.

Topología

Existen dos opciones para implementar una red ETHERNET. La primera consiste en conectar todos los computadores sobre el cable de la red directamente (topología bus). La segunda consiste en utilizar un hub o concentrador, en el cual se conecta cada uno de los cables de red de los computadores.

Tarjeta de red ETHERNET

Cada computador debe tener instalada una tarjeta de red, la cual incorpora los conectores necesarios para que el usuario pueda conectarse al canal. Existen tarjetas ETHERNET de uno o varios conectores. (figura revista N35 pag 47).

Esta tarjeta se debe introducir en el interior del computador. Posee un microprocesador que se encarga de controlar todos los aspectos relacionados con la comunicación y otros como el empaquetamiento y desempaquetamiento de la información que se transmite y recibe, la codificación y decodificación, detección de errores, y en general todas las tareas necesarias para que el computador solamente se preocupe por entregarle la información que se desea transmitir y viceversa.

Cables y conectores que se utilizan

En este tipo de redes se pueden utilizar el cable coaxial, cable UTP y fibra óptica.

El cable coaxial se utiliza sobre todo en la configuración tipo bus, banda base. De esta forma el canal actúa como un mecanismo de transporte, a través del cual se propagan los pulsos digitales de voltaje.

Se utilizan dos tipos de cable coaxial: cable delgado (thin wire) de 0.25 pulgadas de diámetro y cable grueso (thick wire) de 0.5 pulgadas. Por lo general los dos pueden operar a la misma velocidad, 10 Mbps, porque en el cable delgado se presenta una mayor atenuación. La máxima distancia en que se puede transmitir sin necesidad de amplificadores o repetidores es de 200 metros para cable delgado y 500 para el grueso.

Transmisión de información

La red ETHERNET utiliza un protocolo llamado CSMA/CD (Carrier Detect), que quiere decir Acceso múltiple por detección de portadora con detección de colisión.

Como todos los computadores están conectados sobre el mismo bus, se dice que el cable opera en acceso múltiple. Esto significa que cuando un computador quiere mandar información hacia otro computador, debe colocar en el cable todo el paquete de información a ser transmitido. Dicho paquete incluye los datos sobre que usuario los envía y que usuario los recibe, además de la información en sí.

Antes de iniciar, el equipo que va a transmitir debe escuchar el canal para saber que está libre (CS, detección de portadora). En caso de estar ocupado, debe esperar un tiempo y volver a intentarlo nuevamente. En caso de estar libre, puede empezar a transmitir los datos correspondientes.

Como se puede deducir, si dos computadores escuchan el canal al mismo tiempo y éste se encuentra desocupado, empezarán a transmitir sus datos sobre el canal, lo que generará lo que se conoce como colisión de información. En este caso los computadores se retiran por un tiempo y luego cada uno intenta nuevamente hacer su transmisión. Además los computadores que colisionaron colocan una señal en el cable de red que indica que se presentó un choque de datos o información.

Esta es una característica muy importante de este tipo de red, ya que cada computador se retira del canal y no intenta por el contrario, seguir con su transmisión, lo que contribuye notablemente a reducir el tiempo de fallas en la línea. Las tarjetas de red y los transceiver tienen un circuito electrónico que se encarga de realizar las funciones que permiten escuchar el canal y detectar las colisiones.

Formato de la información

Los paquetes de información (también conocidos como tramas) que envía cada computador por la red debe tener un formato específico y cumplir unas normas establecidas, para que sean comprendidas por todos los usuarios de la red. Esas normas cobijan aspectos como la longitud de los paquetes, polaridad o voltaje de los bits, códigos para detección de errores, etc.

(figura pag 48 rev 35) Cada trama empieza con un preámbulo de 7 bytes iguales (10101010). Esto genera una onda cuadrada de 10 MHz, durante un tiempo de 5.6 s, con el objeto de que el receptor se sincronice con el reloj del transmisor. Después viene un byte llamado inicio de trama (10101011), con el fin de marcar el comienzo de la información propiamente dicha.

Los bytes correspondientes a la dirección de destino y de origen se utilizan para saber a quien va el mensaje y quien lo envía. Además, existe un carácter especial que puede indicar que el mensaje va dirigido a un grupo de usuarios o a todos los usuarios. El byte que indica la longitud del campo de datos indica al receptor cuantos bytes de información útil o verdadera debe esperar a continuación. Los datos corresponden al archivo en particular que se está enviando.

Los bytes de relleno se emplean para garantizar que la trama total tenga una longitud mínima de 64 bytes (sin contar el preámbulo ni el inicio de la trama), en caso de que el archivo de datos sea muy corto. Esto se hace con el fin de desechar las tramas muy cortas (menores de 64 bytes) que puedan aparecer en el cable de la red, como consecuencia de transmisiones abortadas por colisiones. El código de redundancia sirve para hacer detección de errores. Si algunos bits de datos llegan al receptor erróneamente (por causa del ruido), es casi seguro que el código de redundancia será incorrecto y, por lo tanto, el error será detectado.

Codificación de los bits. Aunque los bits de información que entrega la tarjeta de red al cable se podrían entregar en forma directa (por ejemplo: 1 voltio para un 1 lógico y 0 voltios para un 0 lógico), esto no le permitiría al receptor saber en que momento empieza cada uno. Además, la potencia que se pierde en el cable sería muy elevada. Por esto, la red utiliza una técnica denominada codificación Manchester, que consiste en asignar dos intervalos de tiempo iguales para cada bit. (figura pag 48 rev 35).

Para representar un uno lógico se tiene que la primera mitad del bit está en nivel alto y la segunda mitad en nivel bajo. Para representar un 0 lógico, el primer intervalo está en nivel bajo y el segundo en nivel alto. Con este esquema se garantiza que cada bit tenga una transición en la parte media, propiciando así un excelente sincronismo entre el transmisor y el receptor.

REDES TOKEN RING

Fue desarrollada por IBM y adoptada por IEEE como estándar IEEE 802.5 en 1986.

Hay tarjetas compatibles de General Instruments, Proteon, 3Com y Ungermann−Bass.

Por definición un "token − ring" consiste en un conjunto de estaciones conectadas en cascada formando un anillo (ring) en el que la información es transferida de una estación activa a la siguiente. Cada estación recibe y regenera los bits que recibe, de forma tal que actúa como repetidor cuando está activa. Cuando la información vuelve a la estación que originó la transmisión, el mensaje es retirado de circulación.

La velocidad de transmisión original era de 4 MBit/s, pero hay versiones de 16 Mbit/s. La codificación es Manchester diferencial. Cuando se desea armar una red Token Ring, lo intuitivo sería pensar en un bus unido por sus extremos. Sin embargo, la topología que aparenta esta red es la de una estrella (se la suele describir como "star − wired ring"). Esto se debe a que el anillo está contenido en un dispositivo denominado Multistation Access Unit (MAU).

Las máquinas se conectan a los pines 1 al 8 del MAU mediante adaptadores (el conector incluído en la tarjeta es distinto al del MAU). Si la red tiene más de 8 puestos, se forma un anillo de MAU conectando la salida de uno (Ring Output, RO) con la entrada del siguiente (Ring Input, RI).

Hay dos formas de cablear el sistema: "small movable cabling system" y "large nonmovable cabling system".En el primer caso, se tienen los siguientes límites:

Hasta 96 estaciones. Hasta 12 unidades MAU. Distancia máxima entre el MAU y una estación: 45,7 m (150 pies) , a los que hay que sumarle 2,4

m (8 pies) del adaptador.

Distancia máxima entre dos MAU: 45, 7 m (150 pies).

No pasar el cable por exteriores ni por conductos de ventilación, no exponerlos a más de 75 grados

Celsius, ni a interferencia eléctrica.

En el segundo caso, se pueden conectar hasta 260 estaciones y 33 MAU, pero se usa un montaje

físico diferente.

Fig. 8 (grafica)

La transmisión se efectúa mediante dos pares trenzados, pero hay de diversas clases, definidas por IBM con números de tipo. El tipo 1 posee 2 pares AWG 22 con blindaje. Se usa principalmente para conectar MAUs. El tipo 2 ofrece 2 pares AWG 22 blindados y 4 pares AWG 26 sin blindaje; los pares extras son para conectar el teléfono con el mismo cable. El tipo 3 es de 2 pares tipo telefónico sin blindar. Es una alternativa barata al tipo 1. La ventaja de usar cable tipo 3 es que en muchas empresas donde hay centrales telefónicas internas, quedan pares disponibles, por lo que no hay que hacer un nuevo tendido; la desventaja es que se limitan el alcance y la cantidad de dispositivos que se pueden soportar (72 en vez de 255). El tipo 6 consta de 2 pares de cables (no alambres) de AWG 26 sin blindaje; es flexible y se usa para los alargues entre el cable adaptador y el MAU. El cable 9 consta de dos pares de AWG 26 blindados. Tiene menor alcance que el tipo 1 (aprox. 66%) pero es más barato. Todos los cables mencionados hasta acá soportan 16 Mbit/s excepto el 3 que llega sólo a 4 Mbit/s.

Por último, el tipo 9 no es un cable sino una fibra óptica. Soporta hasta 250 Mbit/s.

Para ampliar el anillo, se puede usar el 8218 Token − Ring Copper Repeater (repetidor de cobre), llevándolo a 775 m. Otra alternativa es emplear el Token − Ring Network Optical Fiber Repeater (para fibras ópticas), que posibilita enlaces de hasta 2 km.

Hay dos modelos básicos de tarjetas: la Token Ring PC Adapter (para PC, XT, AT, y compatibles) y la Token Ring Adapter/A (TRN/A, para PS/2 Model 50 y superiores).

La diferencia entre ambas es, fundamentalmente, que la primera se conecta en un mainboard con bus tipo XT, mientras que la segunda es para un bus MCA (microchannel).

La dirección de base en el mapa de I/O es A20h (default); se puede escoger IRQ 2, 3 ó 7 (la 7 se superpone con la primera impresora). Un detalle a tener muy en cuenta es que la Token Ring PC Adapter decodifica 12 bits en I/O y no 10 (como es usual en PC).

REDES ARCNET

Fue desarrollada por Datapoint e introducida en 1977. Su nombre es la abreviación de Attached Resource Computing network. Es conocida como un arreglo de redes estrella, es decir una serie de redes estrella se comunican entre sí.

ARCNET se introdujo al mercado de redes como la solución a los problemas presentados por la red tipo estrella, como son la limitación de estaciones de trabajo, separación entre las estaciones de trabajo y el servidor, etc.

ARCNET tiene la facilidad de instalar estaciones de trabajo sin preocuparnos por la degradación de la velocidad del sistema, ya que para tal caso se cuenta con más de un servidor de red.

La no participación en el comité IEEE 802 dio lugar a que ninguna norma 802 la tenga en cuenta. Sin embargo, cuatro factores contribuyeron a hacerla tan popular que es un estándar:

1. a partir de 1982, se comenzaron a vender los chips, por lo que aparecieron "segundas fuentes" de esta tarjeta (Davong, Nestar, Standard Microsystems, Tiara y Waterloo entre otros).

2. el precio es bastante inferior a Ethernet y Token Ring.

3. es muy confiable

4. en muchos lugares de EEUU había cableados con coaxial de 93 ohm en estrella provenientes de hosts con terminales IBM 3270. ARCnet permite que al reemplazar las terminales por computadoras el cableado se aproveche.

En su versión original, es una red con topología tipo estrella, con protocolo de pasaje de "token" , que trabaja en banda base y es capaz de transmitir a 2,5 MBit/s.

Con las tarjetas de interface es posible instalar hasta 128 estaciones de trabajo por cada servidor que se conecte a la red.

Cada una de las estaciones de trabajo puede estar conectada a una distancia máxima de 1200 metros con respecto al servidor de la red, esta distancia equivale a casi el triple de la permitida por la red tipo estrella.

El cable para esta conexión es mucho más caro porque se trata de un RG−62 coaxial que es usado no sólo para conectar esta red entre sí, también utilizado por IBM para la conexión de sus computadoras 3270, esta es otra ventaja, ya que si se cuenta con una instalación de este tipo se puede aprovechar para instalar una red Novell ARCNET.

Una de las grandes ventajas de Novell es el uso de dos tipos de repetidores, el activo y el pasivo, ambas unidades sirven para distribuir la señal de la red entera, de tal forma que una señal determinada llega fácilmente a una estación de trabajo en particular.

Los pasivos consisten en una caja con 4 entradas vinculadas mediante resistores, de valor tal que si tres entradas cualesquiera están terminadas en su impedancia característica, la impedancia vista desde la otra entrada también sea la característica. Esta conexión permite adaptar impedancias y evitar reflexiones, pero a costa de una atenuación alta.

Justamente la atenuación limita la distancia máxima entre cada máquina y el hub a 30 m. Un hub activo, aparte de los resistores de terminación, tiene amplificadores, por lo que se pueden conectar máquinas hasta a 600 m del hub.

Los hubs activos pueden ser internos (generalmente de 4 bocas) o externos (generalmente de 8). Es posible conectar un hub a otro pero se deben respetar estas reglas:

No se pueden conectar hubs pasivos entre sí.

Cualquier entrada no usada en un hub pasivo debe llevar un terminador de 93 ohm.

Ningún cable conectado a un hub pasivo puede tener más de 30 m.

Un hub activo puede estar conectado a una máquina, a otro hub activo o a uno pasivo.

Las bocas no usadas en un hub activo no necesitan terminador, pero es conveniente usarlo.

Tanto los enlaces entre dos hubs activos como los efectuados entre hubs activos y máquinas pueden ser de hasta 600 m.

Ninguna máquina puede estar a más de 6.000 m (20.000 pies) de otra.

No crear ningún lazo.

Para efectuar pruebas entre dos máquinas, no es necesario un hub, se las puede conectar directamente pues las tarjetas poseen terminadores internos.

En la actualidad se la puede considerar obsoleta.

RED ARCNET EN TOPOLOGIA ESTRELLA

Fig. 7

Existen versiones de ARCnet para topología bus y para transmisión por par trenzado, pero no se popularizaron. También se desarrolló una versión denominada "plus" de mayor velocidad de transmisión pero hasta el momento su penetración en el mercado es casi nula.

El chip de control de comunicaciones maneja un buffer de 2 KB y (2048 d = 800 h).

Como ARCnet trabaja con paquetes de longitud fija (508 bytes) y NetWare también (pero de 560 bytes), se requiere transferir dos paquetes ARCnet para transferir un paquete de NetWare (uno de ellos sólo lleva 52 bytes útiles, el resto son 0).

La dirección de la RAM del buffer es seleccionable con jumpers. El default es D0000h − D07FFh, normalmente no interfiere con otras direcciones. La tarjeta también ocupa un espacio de 16 Bytes en el mapa de I/O, siendo el default 2E0 − 2EFh un valor que no interfiere. Emplea una línea de IRQ seleccionable, siendo la 2 por default. En las XT no hay problema, pero en las AT coincide con el IRQ generada por el segundo 8259, por lo que debe cambiarse; las opciones son: 3, 4 (ambas pueden interferir con puertas serie) , 5 y 7 (pueden interferir con puertas paralelo). Por último, hay un par de parámetros de "time − out" que deben seleccionarse mediante DIP switches con la restricción de que deben ser iguales en todas las tarjetas.

<TBODY>	**Ethernet**	**StarLan**	**Token−Ring**	**ARCNET**	**LocalTalk**
IEEE	802.3 10BaseX 10Broad36	802.3 1Base5	802.5	Sin normalizar	Sin normalizar
Método de Acceso	CSMA/CD (aleatorio)	CSMA/CD (aleatorio)	anillo testigo determinista	bus testigo determinista	CSMA/CD (aleatorio)
Origen	1975 Xerox	1982 AT&T	1985 IBM	1980 Datapoint	1984 Apple
Velocidad	10Mbps	1Mbps	4/16 Mbps	2,5 Mbps	230,4 Kbps
Topología	Bus/Estrella	Bus/Estrella	Anil./Estrella	Est./Bu./An.	Bus/Estr.
Medio	Par trenzado, coaxial, fibra óptica	Par trenzado	Par trenzado, fibra óptica	Par trenzado, coaxial, fibra óptica	Par trenzado</TBODY>

TECNOLOGIAS DE ALTA VELOCIDAD

Hoy en día existe una necesidad, cada vez más acuciante, de incrementar el ancho de banda de las redes de área local. El mayor porcentaje de redes de área local instaladas son redes Ethernet (10Mbps) o redes Token Ring (4 o 16 Mbps). Ambas tienen limitaciones importantes:

Las primeras bajan drásticamente su rendimiento cuando crece el número de estaciones conectadas a ellas, llegando a bloquearse a consecuencia del aumento de las colisiones. Las redes Token Ring imponen limitaciones en cuanto al número de estaciones que pueden conectárseles.

Ambas proporcionan anchos de banda suficientes para aplicaciones tradicionales de computador, pero no para las nuevas aplicaciones de tiempo real (transmisión de voz y vídeo) y aplicaciones multimedia que están apareciendo, o bien, para conexiones a servidores de red que están muy solicitados y que necesitan mucho ancho de banda.

El medio de transmisión en las LANs tradicionales (incluida FDDI) es un medio compartido, es decir, hay que competir con el resto de las estaciones para acceder al medio de transmisión. Esto es también ineficaz para las aplicaciones de tiempo real.

Ante esta panorámica se empieza a estudiar la posibilidad de aumentar el ancho de banda de las redes de área local a 100Mbps. Hasta hace muy poco la única tecnología estándar que proporcionaba 100Mbps era FDDI. Sin embargo, la especificación de FDDI, a pesar de superar a todas sus predecesoras, está tardando bastante en entrar en el mercado, incluso en áreas donde en principio tenía grandes ventajas. Esta tardanza se debe, fundamentalmente a dos factores:

Los trabajos originales en la especificación del estándar FDDI comenzaron en 1984, y no finalizaron hasta ocho años después. La tecnología punta no puede esperar tanto.

Los resultados obtenidos han compensado la larga espera, pero no así los costos. A pesar que el rendimiento global de FDDI y la tolerancia a fallos son buenos, FDDI requiere un alto precio inicial en la instalación hardware. Los precios de los interfaces, acopladores, conectores, etc. son muy altos. Además, dada la complejidad del protocolo FDDI, los costos de formación y soporte pueden doblar el precio de la red.

FDDI debería tender a reducir las diferencias de precio que presenta respecto a otros protocolos como 100 BaseT de Fast Ethernet o 100VGAnylan.

ETHERNET Y TOKEN RING A 100Mbps

Se han terminado de desarrollar nuevas tecnologías de Ethernet y Token Ring a 100Mbps. La idea de partida consistió en que los diseños de redes de área local que se plantearán en un futuro próximo estarían basados en bus de FDDI o ATM, usando una tecnología asequible de red local a 100 Mbps, que permitieran que la Ethernet o Token Ring donde trabaja el usuario final tuviera a su disposición un ancho de banda tal que las aplicaciones futuras fueran operativas y no se advirtieran retrasos en su funcionamiento. Se tuvieron que resolver varios problemas. Entre ellos está satisfacer las limitaciones FCC (Federal Communications Commission) de los Estados Unidos, que limitan la radiación emitida por los cables de categoría 3 UTP que lleven tráfico de alta velocidad. En este punto los fabricantes estaban divididos en dos grupos. Para conseguirlo, unos propusieron la propagación de la señal de datos sobre cuatro pares UTP en vez de dos y limitar las transmisiones a un único sentido. El uso de cuatro pares en vez de dos es un requerimiento fácil de cumplir ya que los cableados UTP existentes están hechos con cuatro pares, dos de los cuales no se usan. Sin embargo, la limitación de las transmisiones a un único sentido requeriría la sustitución del mecanismo de acceso al medio CSMA/CD por otro nuevo. Con CSMA/CD las estaciones son capaces de recibir y transmitir datos simultáneamente detectando cuando la red está ocupada. Los opositores sostenían que Ethernet sin CSMA/CD no es Ethernet, y que las limitaciones de las emisiones de radiación deben de superarse usando técnicas de señalización basadas en chips, en vez de reemplazar el mecanismo de acceso al medio. A pesar de los problemas y las diferencias, los grupos de estudio se pusieron de acuerdo en tres puntos cruciales en la tecnología de Ethernet a 100 Mbps: Se debe basar en la misma topología en estrella usada en las redes 10BaseT, con estaciones de trabajo a distancias de hasta 100 metros del HUB.

Debe usar el mismo formato de trama que 10BaseT de forma que para unir las Ethernet existentes con las nuevas a 100 Mbps, sólo hagan falta HUBs equipados con buffers de memoria para manejar la diferencia de velocidades.

Limitar las distancias de la estación de trabajo al HUB a 100 metros, esto hace que no se pueda utilizar como tecnología de bus.

Se formalizarón varias propuestas y algunas de ellas se han establecido como estándar , las más conocidas son: 100BaseVG (IEEE 802.12), 100BaseVG−AnyLAN (IEEE 802.12) y 100BaseT(802.30).

100Base−VG o 100VG−AnyLAN

Es la tecnología de Ethernet a 100 Mbps propuesta por Hewlet Packard y At&T, a la que se unió IBM. En el estándar se propone que las señales sean transmitidas sobre cuatro pares en una única dirección ya sea de estación a HUB o al revés. Fue diseñada con dos objetivos fundamentales:

- Aprovechar la infraestructura de cableado que muchas empresas tienen instalado
- Favorecer aquellas aplicaciones con requerimientos críticos de respuesta en tiempo.

El primer objetivo queda cubierto ya que 100Base−VG tiene una topología en estrella basada en concentradores, y utiliza cuatro pares de hilos que pueden ser UTP de categoría 3 (categoría de voz, de ahí el término VG) o categoría 5 (categoría de datos), STP o bien fibra óptica. La información primero se codifica transformando 5 bits en 6 símbolos (5B/6B) y después éstos se transmiten con señalización NRZ distribuidos en los cuatro canales pues la comunicación es half duplex.

Para satisfacer el segundo objetivo, se propone remplazar CSMA/CD por un nuevo método de acceso llamado Demand Priority Protocol. Con este protocolo las demandas de acceso procedentes de estaciones son enviadas al HUB, encargándose este de responder. Puede funcionar en instalaciones de cableado UTP de categoría 3 (cableado de calidad de voz, o Voice Grade− VG). También se soportan los cableados de categoría 4 y 5. Los conectores que se utilizan son del tipo RJ45, así como los conectores Telco de 50 pines usados para 25 pares de cables. Usando estos conectores y un cable UTP de categoría 3 se pueden soportar las conexiones con distancias entre estación y HUB de 100 metros. Si, en cambio, el cable es de categoría 4 o 5 se soportan distancias de 200 metros y usando conexiones de fibra óptica la distancia puede llegar a ser de 2Km.

Las principales características de 100BaseVG son:

- El formato de la trama en la capa de enlace es idéntico al usado en Ethernet.
- Posee una topología en estrella. Las estaciones están conectadas a un HUB que es un nodo de conmutación de circuitos. Se pueden asignar prioridades a los puertos de dicho HUB.
- Usa los cuatro pares del cable para cada estación (10BaseT solo usa dos). Se divide la señal de 100 Mbps sobre cuatro pares, es decir hay 25 Mbps sobre cada par. De esta forma los niveles de radiación están dentro de los permitidos por las regulaciones FCC. Utiliza un método de codificación llamado 5B6B (5bits en 6 símbolos) para remplazar al método de codificación diferencial Manchester usado en 10BaseT.

El método de acceso (Demand Priority Protocol) actúa de la siguiente manera:

- Una estación emite una petición de transmisión (tono).
- Recibe una autorización de transmisión por parte del HUB (tono).
- El HUB empieza a recibir la trama y mientras determina cual es la estación de destino sigue recibiendo datos (buffer elástico).
- El HUB avisa a la estación de destino del próximo envío de datos.
- La estación destino responde con un preparado para recibir.

- Durante los últimos tres pasos el HUB continua recibiendo datos.
- Se realiza la transmisión de datos al destino (a través de los cuatro pares)
- Ambas estaciones vuelven al estado inicial al terminar la transmisión.

100BaseVG tiene muchas similitudes con respecto a Ethernet, pero implementa varias mejoras:

- Fair Arbitration o acceso determinístico. Se sustituyen las colisiones por un procedimiento determinístico de acceso al medio para cada estación basado en un protocolo de demanda/concesión administrado por el hub. Esto proporciona un ancho de banda ordenado sin colisiones, de forma que el 97% del ancho de banda sea usado por datos de usuario.
- Link Privacy o aislamiento de enlace. El aislamiento del enlace es inherente al protocolo 100BaseVG dado que las estaciones están generando tramas que van por un circuito virtual creado por el hub. Sigue siendo un medio compartido, pues mientras este establecido un circuito no van a poder establecer más. Los paquetes de broadcast se repiten por todos los puertos. La detección de intrusos es muy fácil de implementar con 100BaseVG.
- Demand Priority Signaling o establecimiento de prioridades por demanda. Permite a las aplicaciones multimedia u otras aplicaciones muy sensibles a los retardos aumentar su prioridad de acceso a la red.

Al unirse IBM al grupo de 100BaseVG se cambió el nombre de la especificación por 100BaseVG−AnyLAN. Es una especificación ampliada para permitir que no sólo las tramas Ethernet vaya a 100 Mbps sino también las de Token Ring. Este cambió no retrasó la aparición del estándar ya que incluir dentro de éste formato de las tramas Token Ring no supuso cambios significativos.

Las reglas para la topología y recomendaciones para las redes 100VG−AnyLAN : Regla 1: La topología de red debe ser una estrella física punto a punto, sin ramificaciones ni bucles. Regla 2: En una red 4−pares UTP, se requieren los cuatro pares.

Regla 3: No se usa cable liado UTP (cable que consta de 25 o más pares trenzados en una funda) para los enlaces de redes donde los nodos terminales están configurados en modo promiscuo.

Regla 4: No se usa cable liso en una topología de par trenzado.

Regla 5: Debe haber un único camino activo entre un par de hubs en la red.

Regla 6: La máxima distancia entre un nodo terminal y el hub raíz en una red de segundo nivel es 4 Km. (usando cableado de fibra óptica).

Máximas distancias entre Hub raíz y nodo terminal.−−
Numero de Hubs entre Numero de niveles Máxima distancia entre hub raíz y nodo terminal en la red hub raíz y nodo terminal

−−−

1 2 4 km.

2 3 3 km.

3 4 2 km.

4 5 1 km.

Regla 7: El numero máximo de niveles en una red 100VG−AnyLAN es de 5.

Regla 8: No hay limites en el número de nodos en un segmento no apantallado 100VG−AnyLAN.

Regla 9: Todos los nodos en una porción simple (campo simple a 100 Mbit/s) de una red 100VG−AnyLAN deben usar el mismo formato de paquete soportado por Ethernet/802.3 y token Ring 802.5.

Regla 10: Entre cualquier par de nodos en una red 100VG−AnyLAN, no debería de haber mas de 7 bridges.

Recomendación: Minimizar los niveles de cascada.

100Base−T (Fast Ethernet)

En un principio llamada 100BaseX. Esta especificación fue promovida por Grand Junction, es la evolución de 10BaseT a altas velocidades. 100Base−T utiliza CSMA/CD como protocolo de acceso al medio, transmite tramas con el formato Ethernet a 100 Mbps y emplea una topología de estrella basada en un concentrador. En la capa física existen tres propuestas diferentes: 100Base−TX, 100Base−T4 y 100Base−FX, que permiten utilizar diferentes medios de transmisión. El subcomité 802.3 ha dicho que los esquemas de señalización serán interoperables en una misma red .

Muchas empresas interesadas en desarrollar estas tecnologías formaron una agrupación, The Fast Ethernet Alliance, que entre otras cosas ha logrado presionar al subcomité 802.3 para acelerar los procesos de estandarización. El trabajo original de la propuesta 100Base−TX fue desarrollado por Grand Junction Networks, y a ella se han sumado muchas otras empresas como David Systems, Chipcom, SynOptics, 3Com, Intel, National Semiconductor, DEC y Sun.

100Base−TX consolida dos estándares: el protocolo de acceso al medio CSMA/CD de 802.3 (cambiando únicamente la duración del intervalo entre tramas de 9.6 a 0.96 μs), y la subcapa física dependiente del medio TP−PMD de FDDI. Así, 100Base−TX requiere dos líneas UTP de categoría 5, a través de los cuales transmite con señalización MLT−3, para conectar cada estación al concentrador. Se define una capa de convergencia para mapear la señalización continua full duplex de FDDI con el esquema asíncrono half duplex usado en Ethernet. También puede utilizarse STP como medio físico.

Por otra parte, la tecnología 100Base−T4 es propuesta con el objetivo fundamental de transmitir información a 100 Mbps a través del cableado que se utilizaba hasta 1992 y que se sigue utilizando para redes de voz y de datos a velocidades hasta de 10 Mbps. Este cable es UTP de categoría 3. La especificación sometida a consideración del subcomité 802.3 ha sido desarrollada por SMC, 3Com e Intel.

Utiliza cuatro pares UTP (de ahí el término T4), tres pares se utilizan para transmitir o recibir la trama (la comunicación es half duplex) mientras que el último par se utiliza exclusivamente como entrada para detección de colisiones. Antes de ser transmitidos, los datos se codifican transformando 8 bits en 6 símbolos ternarios (8B/6T). La información ternaria es entonces transmitida por los canales de datos. Este modelo es técnicamente similar a la señalización MLT−3, ofreciendo un nivel adecuado de emisiones electromagnéticas.

Por último, la propuesta 100Base−FX emplea dos fibras ópticas multimodales.

Al igual que en 10BaseT, la distancia máxima entre una estación y el concentrador en 100Base−T es de 100 metros. Sin embargo, las reglas de topología permitidas son diferentes en 100Base−T: sólo se permiten dos repetidores, y la distancia máxima de una red es de 205 metros si se utiliza par trenzado y 325 si se emplea fibra óptica .

FDDI. UNA RED DE FIBRA OPTICA

FDDI (Fiber Distributed Data Inteface) es una evolución de Ethernet, token bus a protocolos de mayores prestaciones. Propuesto por ANSI (standard X3T9.5). Hacia 1980, comienzan a necesitarse redes que transmitan datos a alta velocidad.

También se necesitaba transmitir datos en tiempos cortos y acotados. En respuesta a estas necesidades, se desarrolla FDDI. FDDI ofrece 100 Mbps, con hasta 500 estaciones conectadas y un máximo de 100 km entre ellas. Las estaciones se conectan en un doble anillo de fibra óptica por seguridad. Por su alta velocidad de transmisión, también puede usarse como una red de conexión entre redes más pequeñas.

Funciones de FDDI

Las funciones de FDDI se define en el SMT (Station ManagemenT). Abarcan la capa física (PMD y PHY) y parte de la capa de enlace (MAC). Por ello, FDDI se instala en los niveles más bajos de la torre OSI. No habría problemas en usar otros protocolos para las capas superiores, en principio. Por lo contrario, las implementaciones sólo han conseguido encapsular correctamente ARP e IP sobre FDDI.

Nivel Físico: PMD

En el nivel dependiente del medio (PMD), FDDI no impone restricciones al tipo de fibra que debe usarse. Puede utilizarse fibra multimodo (MMF), o fibra monomodo (SMF). Las fibras serán de dimensiones 62,5/125 o 85/125 (diámetro del núcleo/di metro de la fibra). MMF necesita mejores emisores y receptores que SMF para mantener las mismas longitudes de enlace. En cualquier caso, la potencia de transmisión mínima es de −16 dBm y la potencia recibida mínima es de −26 dBm, lo que deja un margen de 11 dBs para pérdidas. Los transmisores pueden ser LED o láseres. Los receptores pueden ser diodos PIN o de avalancha. Se trabaja en la ventana de 1300 nanómetros. En una misma red puede haber enlaces con fibras MMF y SMF, aunque deben examinarse con cuidado. Se recomienda emplear conectores SC preferentemente. También pueden emplearse conectores ST. La probabilidad de error requerida es 4*10−11.

Nivel Físico: PHY

El otro subnivel físico, PHY, define el protocolo de introducción de datos en la fibra. FDDI introduce redundancia en los datos en transmisión. Usa un código 4B/5B, transmite 5 bits por cada 4 bits que le envía el nivel superior. La elección de los códigos se hizo para equilibrar la potencia continua del código, y evitar secuencias de 0's o 1's demasiado largas. El régimen binario efectivo que soporta la fibra son 125 Mbps.

MAC define la longitud máxima de trama en 4500 bytes para evitar problemas de desincronización. No hay longitud de trama mínima. El formato de trama es:

PA = Preámbulo: 30 caracteres IDLE, para sincronismo.

SD = delimitador de inicio. No se repite en el campo de datos. FC = control de trama. Tipo de trama (síncrona, etc.). DA = Dirección de destino.

SA = Dirección de destino.

INFORMACION: Datos transmitidos.

FCS= Redundancia de la trama con CRC−32.

ED = Delimitador de fin de trama. No se puede repetir en el campo de datos.

FS = Frame Status. Receptor informa a origen del resultado de la trama (trama errónea, bien recibida, etc.)

Una estación que está transmitiendo trama debe retirarla del anillo. Mientras lo hace, puede introducir nuevas tramas, o transmitir caracteres IDLE, hasta retirarla completamente. Dado que protocolos superiores (UDP, por ejemplo) definen longitudes de trama diferentes, las estaciones deben estar preparadas para fragmentar/ensamblar paquetes cuando sea necesario.

Nivel de enlace: MAC

MAC aporta las mayores novedades de FDDI. FDDI soporta dos tipos de tráfico:

* Tráfico síncrono: voz, imágenes, etc., información que debe ser transmitida antes de un determinado tiempo. Podría decirse que es tráfico de datos en tiempo real.

* Tráfico asíncrono: e−mail, ftp, etc., información para la cual el tiempo que tarde en llagar al destino no es el factor decisivo.

La filosofía que persigue FDDI es atender primero el tráfico síncrono y después el tráfico asíncrono. Para ello, cada estación tiene varios temporizadores:

* Token Rotation Time (TRT): tiempo transcurrido desde que llegó el último testigo.

* Token Hold Time (THT): tiempo máximo que una estación puede poseer el testigo.

Todas las estaciones tienen un parámetro fijo, el Target Token Rotation Time (TTRT), que fija el tiempo que tarda el testigo en dar una vuelta al anillo, y cada una tiene un parámetro propio, Syncronous Time (ST o Ci, dependiendo de autores). Este parámetro fija el tiempo máximo que una estación está transmitiendo tráfico síncrono.

Cuando llega el testigo, comprueba que ha llegado a tiempo. Para ello, ve si TRT > 0. Si es cierto, la estación captura el testigo. Si es falso, la estación la estación lo deja pasar a la siguiente estación. En cualquier caso, TRT se reinicializa a TTRT.

2) Una vez la estación posee el testigo, el valor de TRT se carga en THT. Se comienzan a transmitir tramas síncronas.

3) THT llega a cero. En ese caso, se termina el turno de la estación, y se pasa el testigo a la siguiente.

4) Antes de que THT llegue a 0 se acaban las tramas síncronas que tenía la estación preparada para transmitir. Se transmiten ahora todas aquellas tramas asíncronas de que se dispongan, hasta que THT llegue a cero.

5) Si se acaba también las tramas asíncronas, pasa el testigo.

Se plantea un problema cuando se acaba el THT mientras se está transmitiendo una trama. Este fenómeno se llama overrun.

El intervalo máximo entre dos testigos en una estación ronda 2*TTRT.

Las estaciones se conectan mediante un doble anillo de fibra óptica. En cada anillo, la información circula en una dirección. En caso de que caiga un enlace entre dos estaciones, las fibras se puentean internamente en las estaciones, de modo que el anillo no se para. Esta configuración clasifica las estaciones en dos clases:

* DAS : Dual Attachment Station. Estación conectada al doble anillo. Capaces de reconfigurarse. Más caras.

* SAS : Single Attachment Station. Estación conectada a uno de los dos anillos solamente. Más baratas.

Otras soluciones alternativas

Se han planteado otras soluciones al standard original expuesto anteriormente. Todas las soluciones se basan en el estándar FDDI, aunque varían algunos niveles, para adaptarlo a determinadas situaciones. Las soluciones más atractivas son CDDI, FDDI−II, y LCF−FDDI

CDDI

CDDI (Copper Distributed Data Interface) no es otra cosa que FDDI utilizando cables de cobre en lugar de fibra óptica como medio de transmisión. Sólo afecta al PMD. Para seguir cumpliendo los requerimientos de ruido y velocidad de transmisión se reduce la distancia máxima de enlace a 100 m. Para evitar también la radiación que produce el par trenzado sin blindaje (Unshielded Twisted Pair, UTP) cuando se utilice este medio de transmisión se utiliza un código diferente, NRZ− III. Básicamente, es NRZ con tres niveles, subiendo y bajando niveles hasta llegar a los extremos. De este modo, baja la frecuencia máxima que soporta el par trenzado, reduciéndose las radiaciones. La principal ventaja que aporta CDDI es la reducción en los costos de implantación de FDDI, sobre todo cuando se quiere hacer llegar FDDI hasta los terminales de usuario (FDDI− on−desk). Los terminales suelen estar ya cableados, por lo que sustituir el cobre por la fibra óptica aparece como un costo innecesario en muchos casos. Además, los receptores y transmisores ópticos que emplea FDDI resultan demasiado caros frente a los dispositivos electrónicos que utiliza CDDI. Por lo demás, los cambios en el código no son relevantes y la reducción en la distancia máxima no es importante, puesto que CDDI se utilizaría dentro de los edificios, en los que las distancias suelen ser inferiores a esos 100 metros críticos.

FDDI−II

FDDI−II cambia el servicio que ofrece. Amplía SMT hasta completar el nivel de enlace. Ahora el nivel de red no ve un único canal de 100 Mbps sino que este canal se divide en 16 canales isócronos de 6,144 Mbps (WBC), y un canal de transmisión de paquetes, de 768 Kbps (PDG). Las tramas son de 0.125 ms y contienen intercalados los distintos canales. Inicialmente, se envían 2,5 bytes de preámbulo que sincronizan el reloj de 8 Khz que inicia las tramas y 12 bytes de cabecera de la trama. Se envía el byte correspondiente al PDG. Luego se envía un byte de cada canal. Cuando se llega a un byte múltiplo de 8 en los WBC se vuelve a enviar 1 byte de PDG.

Usualmente, los testigos se pasan a través del PDG. Los WBC pueden subdividirse en canales menores, en funciones de las necesidades de las estaciones.

Aparece ahora un nuevo tipo de tráfico, de prioridad mayor que el síncrono de FDDI, que es el tráfico conmutado. Hay dos testigos, testigo restringido y testigo sin restricciones. Dependiendo de las restricciones en tiempo de llegada de las tramas se utiliza una combinación de tráfico y testigos.

LCF−PMD

LCF−PMD (Low−Cost Fiber Physical Medium Dependent) surge también como necesidad económica. Se busca reducir el costo de implantación de una red FDDI. Para ello, se cambia de nuevo el PMD. Se introduce unos nuevos tipos de fibra (200/230), más baratos y de peores prestaciones. Igual que en CDDI, se amplían los márgenes de ruido, y se reducen las longitudes de los enlaces, ahora hasta los 500 metros. Se reduce la potencia mínima de transmisión en 2 dBm. Se relaja en 2 dBm la potencia mínima de recepción, quedando sólo 7 dBs para pérdidas. El resto del protocolo no se altera.

Rendimiento

El rendimiento de FDDI se mide en dos aspectos: Retardo de as tramas en llegar a la estación destino y cantidad de datos que llegan a destino por segundo. Un primer par metro de importancia es el TTRT. Si es pequeño, el testigo circula muy rápidamente, de modo que el retardo es pequeño. Si es grande, el desempeño es mayor, pero estaciones con mucha carga retrasan a las demás. Los valores típicos de TTRT rondan los 4 ms o los 165 ms,. Otro factor a tener en cuenta es el tamaño de los paquetes. Si es grande, aumenta el desempeño. Si es pequeño, disminuye el retardo.

Conclusiones

En conclusión, FDDI ofrece transmisión de datos a alta velocidad, en tiempo real o no, entre un número de estaciones alto y separadas una distancia elevada. También puede servir como red de conexión entre LANs que estén funcionando previamente. Se ha sabido adaptar a las características de entornos en los que resulta muy deseable disponer de ella, pero su elevado costo inicial parecía prohibir. Esto hace de FDDI y LCF alternativas muy interesantes para LANs. Sin embargo, la irrupción de ATM ha hecho que FDDI se considere "la hermana pequeña" de las redes de comunicación óptica. ATM ha hecho que FDDI ya no sea un campo de investigación tan activo como fue a finales de los 80, ni siquiera en FDDI−II, que aprovecha parte de las ideas que utiliza ATM. Por ejemplo, la inclusión de canales virtuales conmutados.

ATM

ATM se originó por la necesidad de un standard mundial que permitiera el intercambio de información, sin tener en cuenta el tipo de información transmitida. Con ATM la meta es obtener un standard internacional. ATM es una tecnología que va creciendo y es controlada por un consenso internacional, no por la simple vista o estrategia de un vendedor.

Desde siempre, se han usado métodos separados para la transmisión de información entre los usuarios de una red de área local (LAN) y los de una red de gran tamaño(WAN). Esta situación traía una serie de problemas a los usuarios de LAN's que querían conectarse a redes de área metropolitana, nacional y finalmente mundial. ATM es un método de comunicación que se puede implantar tanto en LAN's como en WAN's. Con el tiempo, ATM intenta que las diferencias existentes entre LAN y WAN vayan desapareciendo.

Actualmente se usan redes independientes para transportar voz, datos e imágenes de video debido a que necesitan un ancho de banda diferente. El tráfico de datos no necesita comunicar por un periodo extenso de tiempo sino transmitir grandes cantidades de información tan rápido como sea posible. Voz y video, por otra parte, tienden a necesitar un trafico mas uniforme siendo muy importante cuando y en el orden en que llega la información. Con ATM, redes separadas no serán necesarias. ATM es el única tecnología basada en estándar que ha sido diseñada desde el comienzo para soportar transmisiones simultaneas de datos, voz y video.

ATM es un standard para comunicaciones que esta creciendo rápidamente debido a que es capaz de transmitir a una velocidad de varios Megabits hasta llegar a Gigabit.

Cuando se necesita enviar información, el emisor "negocia" un camino en la red para que su comunicación circule por él hacia el destino. Una vez asignado el camino, el emisor especifica el tipo, la velocidad y otros atributos de la comunicación.

Otro concepto clave es que ATM está basado en el uso de conmutadores. Hacer la comunicación por medio de un conmutador (en vez de un bus) tiene ciertas ventajas:

Reserva de ancho de banda para la conexión

Mayor ancho de banda

Procedimientos de conexión bien definidos

Velocidades de acceso flexibles.

Si se usa ATM, la información a enviar es dividida en paquetes de longitud fija.

Estos son mandados por la red y el destinatario se encarga de poner los datos en su estado inicial. Los paquetes en ATM tienen una longitud fija de 53 bytes, esto permite que la información sea transportada de una manera predecible. El hecho de que sea predecible permite diferentes tipos de trafico en la misma red.

Los paquetes están divididos en dos partes, la cabecera y payload. El payload (que ocupa 48 bytes) es la parte del paquete donde viaja la información, ya sean datos, imágenes o voz. La cabecera (que ocupa 5 bytes) lleva el mecanismo direcccionamiento.

ATM a pasado de la teoría a la realidad con productos y servicios disponibles hoy en día. EL ATM forun ha patrocinado demostraciones de interoperatibilidad para demostrar la tecnología y continua reuniéndose para discutir sobre la evolución de ATM.

EL ATM coexiste con la actual tecnología LAN/WAN. Las especificaciones de ATM están siendo descritas para asegurar que el ATM integre las numerosas tecnologías de red existentes, a varios niveles(ie, Frame Relay, Ethernet, TCP/IP).

Equipos, servicios y aplicaciones están disponibles hoy en día y están siendo actualmente usadas en redes.

La industria de la telecomunicación se dirige al ATM.

Paquetes ATM:(ojo gráfica)

Un paquete en ATM es la información básica transferida en las comunicaciones B−ISDN de ATM. Los paquetes tienen una longitud de 53 bytes. Cinco de estos bytes forman la cabecera y los 48 bytes que quedan forman el campo de información del usuario llamado "payload". Durante el proceso de estandarización aparecieron problemas a la hora de determinar la longitud de los payload de los paquetes. Por una parte en USA se preferían unos payload de 64 bytes ya que parecía ser mas adecuado para el funcionamiento de sus redes. Por otra parte los europeos y japoneses querían payload de 32 bytes para el mejor funcionamiento de sus redes. Al final se opto como compromiso los 48 bytes actuales que mas los 5 bytes que ocupa la cabecera forman los 53 bytes de cada paquete.

La siguiente estructura corresponde a la cabecera de un paquete NNI:

(ojo imagen)

La siguiente estructura corresponde a la cabecera de un paquete UNI:

(ojo imagen)

La cabecera se divide en los campos GFC, VPI, VCI , PT, CLP y HEC. Los tamaños de estos campo difieren mínimamente entre el NNI y el UNI. Los tamaños de los campos son los siguientes:

(ojo imagen)

Los Standards de ATM especifican que los paquetes de ATM deben ser enviados en orden. Cualquier switch y equipo diseñado deberá tener esto en cuenta.

Paquetes de ATM

La longitud de los paquetes en ATM es de 53 bytes. Los primeros 5 bytes corresponden a la cabecera y los restantes 48 al payload:

<−−−−−−−−−−−−− 5 bytes −−−−−−−−−−−−−−−−>|<−−−−−−−−−− 48 bytes −−−−−−−−−>|

−−−

| VCI Label | control | header checksum | optional adaptation | payload |

| 24 bits | 8 bits | 8 bits | layer 4 bytes |44 or 48 |

−−

Control de Flujo Genérico (GFC):

Aunque la función primaria de este campo es el control del acceso físico, a menudo se usa para reducir celda en servicios CBR, asigna capacidad de feria para servicios VBR, y para hacer control de trafico en flujos VBR.

Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI):

La función de los campos VPI/VCI es indicar el numero de canal/camino virtual, por lo cual los paquetes que pertenezcan a la misma conexión pueden ser distinguidos. Se asigna un único VPI/VCI para indicar el tipo de paquete que viene, paquetes sin asignar, paquetes OAM de la capa física.

ATM es un protocolo orientado a conexión las cuales tienen un identificador de conexión en cada cabecera de los paquetes que asocia un paquete con un canal virtual dado en una conexión física. Este identificador esta compuesto por dos campos: VPI y VCI. Juntos son usados para multiplexar y demultplexar los paquetes en la red. Estos campos no son direcciones. Son asignados explícitamente en cada segmento (conexiones entre los nodos ATM) de una conexión cuando una conexión se establece y duran mientras la conexión permanece. Usando VCI/VPI la ATM layer puede tratar paquetes de distintas conexiones.

Cada conexión en una red ATM puede ser dividida en dos partes, una en cada dirección. Cada parte tiene su propio VCC por lo que en este contexto VP y VC pueden ser considerados como unidireccionales.

Sin embargo, uno siempre encuentra los mismos VPI/VCI en ambas direcciones para una conexión. Esto puede ser considerado como una limitación o una simplificación en las especificaciones.

Tampoco hay ningún hecho que nos diga que el mismo ancho de banda debe ser encontrado en ambas direcciones. De hecho, tiene un trafico independiente y cada dirección tiene sus propios parámetros. Algunas conexiones pueden asignar los mismos parámetros para ambas direcciones si los dos tráficos son simétricos pero esto no es obligatorio.

Con independencia de lo anterior, relativo a la implementación, VP y VC deben ser bidireccionales.

Payload Type (PT)/Cell Loss Priority (CLP)/Header Error Control (HEC):

El campo PT deberá informar si la información del usuario ha llegado o los paquetes ATM han sufrido congestión.

El campo CLP se usa para decir al sistema si el paquete debe ser descartado o no en momentos de congestión. Los paquetes ATM con CLP= 0 tienen una prioridad menor que los paquetes ATM con CLP= 1. Por lo tanto, cuando se produce congestión, los paquetes que tienen el campo CLP= 1 antes son quitados antes que los que tienen el campo CLP= 0.

HEC es un byte de CRC de la cabecera que es usado para detectar y corregir errores en los paquetes.

Arquitectura de ATMATM es una arquitectura estructurada en capas que permite que múltiples servicios como voz y datos vayan mezclados en la misma red. Tres de las capas han sido definidas para implementar los rasgos del ATM.

La capa de adaptación garantiza las características apropiadas del servicio y divide todos los tipos de datos en payload de 48 bytes que conformaran el paquete ATM.

La capa intermedia de ATM coge los datos que van a ser enviados y añade los 5 bytes de la cabecera que garantiza que el paquete se envía por la conexión adecuada.

La capa física define las características eléctricas y los interfaces de la red. ATM no esta ligado a un tipo especifico de transporte físico.

Beneficios ATM:

Una única red ATM dará cabida a todo tipo de trafico(voz, datos y video).ATM mejora la eficiencia y manejabilidad de la red.

Capacita nuevas aplicaciones−debido a su alta velocidad y a la integración de los tipos de trafico, ATM capacitara la creación y la expansión de nuevas aplicaciones como la multimedia.

Compatibilidad−porque ATM no esta basado en un tipo especifico de transporte físico, es compatible con las actuales redes físicas que han sido desplegadas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.

Simplifica el control de la red−ATM esta evolucionando hacia una tecnología standard para todo tipo de comunicaciones. Esta uniformidad intenta simplificar el control de la red usando la misma tecnología para todos los niveles de la red.

Largo periodo de vida de la arquitectura−Los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizando el ATM. ATM ha sido diseñado desde el comienzo para ser flexible en:

Distancias geográficas

Numero de usuarios

Acceso y ancho de banda(hasta ahora, las velocidades varían de Megas a Gigas).

La capa de adaptación de ATM:

Para que ATM pueda soportar distintos tipos de servios con tráficos diferentes, es necesario adaptar estas

aplicaciones a la ATM layer. Esta función es desarrollada por el AAL que es un servicio que depende del cliente.

La capa de Adaptación de ATM yace entre el ATM layer y las capas más altas que usan el servicio ATM. Su propósito principal está en resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles del ATM layer. La capa de adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes :

1) Que la información que esta siendo transportada dependa o no del tiempo.

2) Tasa de bit constante/variable.

3) Modo de conexión.

Estas propiedades definen ocho clases posibles, cuatro se definen como B−ISDN Clases de servicios. La capa de adaptación de ATM define 4 servicios para equiparar las 4 clases definidas por B−ISDN:

AAL−1

AAL−2

AAL−3

AAL−4

La capa de adaptación se divide en dos subcapas:

1)Capa de convergencia

En esta capa se calculan los valores que debe llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.

2)Capa de Segmentación y reensamblaje:

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

AAL1:

AAL−1 se usa para transferir tasas de bits constantes que dependen del tiempo.

Debe enviar por lo tanto información que regule el tiempo con los datos. AAL−1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada.

Capa de convergencia:

Las funciones provistas a esta capa difieren dependiendo del servicio que se proveyó. Provee la corrección de errores.

Capa de segmentación y reensamblaje: En esta capa los datos son segmentados y se les añade una cabecera. La cabecera contiene 3 campos (ver diagrama)

ALL 2:

AAL−2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL−2 provee recuperación de errores e indica la información que no puede recuperarse.

Capa de convergencia:

Esta capa provee para la corrección de errores y transporta la información del tiempo desde el origen al destino.

Capa de segmentación y recuperación:

El mensaje es segmentado y se le añade una cabecera a cada paquete. La cabecera contiene dos campos.

Numero de secuencia que se usa para detectar paquetes introducidas o perdidas.

El tipo de información es:

BOM, comenzando de mensaje

COM, continuación de mensaje

EOM, fin de mensaje o indica que el paquete contiene información de tiempo u otra.

El payload también contiene dos campos:

Indicador de longitud que indica el numero de bytes validos en un paquete parcialmente lleno.

CRC que es para hacer el control de errores.

AAL 3:

AAL−3 se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL−3 puede ser dividido en dos modos de operación:

1) Fiable: En caso de perdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.

2) No fiable: La recuperación del error es dejado para capas mas altas y el control de flujo es opcional.

Capa de convergencia:

La capa de convergencia en AAL 3 es parecida al ALL 2. Esta subdividida en dos secciones

1)Parte común de la capa de convergencia. Esto es provisto también por el AAL−2 CS. Añade una cabecera y un payload a la parte común (ver diagrama)

La cabecera contiene 3 campos:

Indicador de la parte común que dice que el payload forma parte de la parte común.

Etiqueta de comienzo que indica el comienzo de la parte común de la capa de convergencia.

Tamaño del buffer que dice al receptor el espacio necesario para acomodar el mensaje.

El payload también contiene 3 campos:

Alineación es un byte de relleno usado para hacer que la cabecera y el payload tengan la misma longitud.

Fin de etiqueta que indica el fin de la parte común de la CS(capa de convergencia).

El campo de longitud tiene la longitud de la parte común de la CS.

2) Parte especifica del servicio. Las funciones proveídas en esta que capa dependen de los servicios pedidos. Generalmente se incluyen funciones para la recuperación y detección de errores y puede incluir también funciones especiales.

Capa de segmentación y reensamblaje

En esta capa los datos son partidos en paquetes de ATM. Una cabecera y el payload que contiene la información necesaria para la recuperación de errores y reensamblaje se añaden al paquete. La cabecera contiene 3 campos:

1) Tipo de segmento que indica que parte de un mensaje contiene en payload.

Tiene uno de los siguientes valores:

BOM: Comenzando de mensaje

COM: Continuación de mensaje

EOM: Fin de mensaje

SSM: Mensaje único en el segmento

2) Numero de secuencia usado para detectar una inserción o una perdida de un paquete.

3) Identificador de multiplexación. Este campo se usa para distinguir datos de diferentes comunicaciones que ha sido multiplexadas en una única conexión de ATM.

El payload contiene dos de campos:

1) Indicado de longitud que indica el número de bytes útiles en un paquete parcialmente lleno.

2) CRC es para el control de errores.

ALL 4:

AAL−4 se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y o fiable. AAL−4 provee la capacidad de transferir datos fuera de una conexión explícita.

AAL5 es un mecanismo para partir y volver a unir mensajes. Son unas normas que tanto el que envía el

mensaje como el que lo recibe las usan para coger un mensaje y dividirlo en paquetes. El que envía el mensaje tiene como misión construir el conjunto de paquetes que van a ser enviados. La función del receptor será recoger todos los paquetes, verificar que se han recibido sin errores y juntarlos para formar el mensaje original.

Relación entre ATM y B−ISDN:

Se puede resumir en una frase: ATM hace posible el B−ISDN en una realidad. Esto no nos da una idea acertada de la relación. El ISDN (Integrated services Digital Network) se desarrollo durante los 80's. Tomo una canal básico que podía operar a 64kbps (canal B) y combinaciones de otros (canales D) para formar la base para las redes de comunicaciones.

Sin embargo, al mismo tiempo, la demanda de comunicaciones a alta velocidad (FDDI LAN and DQDB LAN) y comunicaciones de video aumentaba rápidamente.

Por esto se creo Broadband−ISDN la cual solo es una extensión de ISDN por lo cual las funciones de comunicación entre redes, video teléfono, videoconferencia, etc., son tratadas como en el ISDN tradicional. Esta diversidad de servicios precisa unas velocidades de 155Mbps, 622Mbps y 2.4Gbps y unas determinadas transmisiones y conexiones para esas velocidades. Mientras que SDH se usaba para las transmisiones, la conmutación de paquetes apareció como la solución al problema de las conexiones. Las relaciones entre ATM y B−ISDN se muestran en el siguiente diagrama:

Las conexiones para broadband no son sencillas de realizar debido a la necesidad unos anchos de banda de varias decenas de bps que pueden llegar a 100 Mbps para transmitir ciertas señales. Esto nos puede llevar entre varios segundos a varias horas. Como ATM resuelve estos problemas, B−ISDN puede existir como una realidad y llegar a ser implementado en un futuro en redes.

Control de Trafico en ATM Una red ATM necesita tener unas capacidades para controlar el trafico dando cabida a las distintas clases de servicios y a superar posibles errores que se pueden producir dentro de la red en cualquier tiempo. (Ej. : Un problema con la capa física). La red tiene que tener las siguientes capacidades para controlar el trafico.

Recursos de dirección de la red Control de admisión de una conexión Uso de parámetros de control y de parámetros de control de red Control de Prioridad Control de Congestión

Procedimientos de Control de Trafico y su impacto en la dirección de la red

Los procedimientos de control de trafico en redes ATM actualmente no están completamente estandarizados. Pero la meta de estos procedimientos es, conseguir una buena eficiencia en la red dar calidad al servicio requerido por el usuario con un método que es generalmente aplicable. Por lo tanto, unos controles de trafico mas sofisticados y unas acciones para los recursos de la red están siendo tenidas en cuenta.

El problema fundamental en las redes ATM es el comportamiento de los paquetes en los procesos de llegada. Se ha visto que la calidad del servicio depende mucho de este comportamiento. Por lo tanto, es necesario usar modelos de trafico para evaluar la ejecución.

Recursos de dirección de la red

Un instrumento de recurso de dirección de la red que puede ser usado para el control de trafico es la técnica de los caminos virtuales. Agrupando varios canales virtuales un camino virtual, otras formas de control pueden ser simplificadas (ej. cac y upc). Los mensajes para el control de trafico pueden ser mas fácilmente distribuidos en un canal virtual que estará dentro de un camino virtual.

Control de admisión de una conexión

El control de admisión de una conexión es la colección de acciones tomadas por la red durante la fase de instalación para establecer si un camino/canal virtual puede ser aceptado por la red.

Una conexión solo puede ser establecida si los recursos disponibles de la red son suficientes para establecer la conexión con la calidad que requiere el servicio. La calidad de servicio de los canales existentes no debe ser afectada por la nueva conexión.

Dos clases de parámetros están previstos para mantener el control de admisión de una conexión:

Un conjunto de parámetros que describen las características del trafico en el origen.

Otro conjunto de parámetros para identificar la calidad que el servicio requiere.

Uso de parámetros de control y parámetros de control de la red

El uso de parámetros de control (UPC) y los parámetros de control que tiene la red (NPC) hacen la misma función en diferentes interfaces. La función de los UPC es desarrollada en las interfaces del usuario, mientras que la función de los NPC se realiza en los nodos de la red.

El propósito principal de los UPC/NPC es proteger los recursos de la red ya que se puede llegar a afectar la calidad de servicio de otra conexión ya establecida.

El uso de parámetros supervisores incluye las siguientes funciones:

Verificar la validez de los valores de los VPI/VCI.

Supervisión del volumen de trafico de la red.

Supervisión de todo el volumen de trafico aceptado en un nuevo acceso.

El uso de parámetros de control puede simplificar el rechazo de paquetes que llevan errores en sus parámetros de trafico. Una medida menos rigurosa puede consistir en marcar los paquetes erróneos y dejarlos en la red si no causan daño.

Control de PrioridadLos paquetes de ATM tienen un bit de prioridad de perdida en la cabecera del paquete así el cual puede tomar por lo menos dos valores diferentes. Una conexión sencilla de ATM puede tener ambos valores cuando la información transmitida esta clasificada en partes mas o menos importantes.

Control de congestión

El control de congestión es un estado de los elementos de la red en el cual el trafico sobrepasa los recursos de la red y esta no es capaz de garantizar la calidad de los servicios a las conexiones establecidas.

El control de congestión es un medio de minimizar los efectos de la congestión impidiendo que estos se propaguen. Puede emplear CAC y/o UPC para evitar situaciones de congestión.

Canales/Caminos Virtuales

ATM provee dos tipos de conexiones para el transporte de datos: Caminos virtuales y Canales virtuales. Un canal virtual es una tubería unidireccional formado por la suma de una serie de elementos de la conexión. Un

camino virtual esta formado por una colección de estos canales (vea diagrama) Cada camino y cada canal tienen un identificador asociado. Todos canales dentro de un camino sencillo tienen que tener un identificador de canal distinto pero pueden tener el mismo identificador de canal si viajan en caminos diferentes. Un canal individual puede por lo tanto ser inequívocamente identificado por su numero de canal virtual y por el numero de camino de virtual.

El numero de canal y camino virtual de una conexión puede diferir del origen al destino si la conexión se conmuta dentro de la red. Los canales virtuales que queden dentro de un camino virtual sencillo en una conexión tendrá n los mismos identificadores de canales virtuales. La secuencia de paquetes es mantenida a través de un canal virtual. Cada canal y camino virtual han negociado un QOS asociado. Este par metro incluye valores para controlar la perdida y retardo de paquetes.

STM

ATM es el complemento de STM cuyo significado es Modo de Transmisión Sincrona. El STM es usado en las redes de telecomunicaciones para transmitir paquetes de datos y voz a lo largo de grandes distancias. La red esta basada en la tecnología de conmutadores donde una conexión es establecida entre dos puntos antes de que la transmisión de datos comience. De esta forma, los puntos finales localizan y reservan un ancho de banda para toda la conexión. El ancho de banda de la red STM es dividido para las distintas conexiones y estas a su vez se dividen en unidades mínimas de transmisión llamadas cubos. Estos cubos se juntan formando colas que tienen un numero fijo de cubos etiquetados de 1 a N. Estas colas son mandadas en unidades de tiempo T siempre manteniendo el orden y las etiquetas de los cubos. Puede haber M diferentes colas numeradas de 1 a M en un mismo periodo de tiempo T. Los parámetros N, M y T están especificados en estándares y son diferentes en Europa y en América.

En una conexión STM entre dos puntos finales, se asigna un numero fijo de cubos numerados de 1 a N, un numero fijo de colas numeradas de 1 a M, y la forma en que los datos viajan en los cubos de la cola. Si hay nodos intermedios, es posible que un numero diferente de cubos sea asignado a una cola de una conexión STM. Sin embargo, siempre hay un cubo inicial para cada conexión que nos indica la información referente a esa cola.

NORMAS

NORMA IEEE 802.3

A finales de los años 70 y principios de los 80, dentro del organismo internacional IEEE, se desarrollaron varias especificaciones técnicas relativas a las redes de área local, que iban a dar lugar a unos estándares. Entre éstos está Ethernet.

Ethernet utilizaba en sus inicios como soporte físico dos tipos de cable coaxial: el Thicknet definido por la norma 10Base5, y el Thin−net, definido por la norma 10Base2. Popularmente coaxial grueso y fino respectivamente. Este soporte físico se utiliza con una topología tipo bus, y a una velocidad de transmisión de 10 Mbps. Se utiliza una codificación de datos Manchester.

Las estaciones conectadas a la red ejecutan un protocolo que regula el acceso al medio. Este protocolo es el CSMA/CD. Según este protocolo, cada estación que desea transmitir comprueba primero si el bus está libre, si es así, envía una trama a la estación destino. La trama contiene la dirección de destino, la de origen, el tipo de trama, los datos a transmitir y cuatro bytes para comprobación de errores. El tamaño máximo de una trama es de 1500 bytes. Cada computador tiene su dirección Ethernet (o dirección MAC), que es única y se encuentra codificada en el hardware del interface de red. Si dos o más estaciones intentan transmitir por el bus a la vez, pues realizan la comprobación al mismo tiempo, se produce una colisión. Las estaciones detectan esta colisión (pues lo que escuchan no es lo mismo que lo que han enviado) y esperan un tiempo aleatorio, diferente en

cada una, antes de reintentar el envío. La principal ventaja de este método de acceso es que, en condiciones de carga baja de la red, se garantiza el envío instantáneo de las tramas. Pero en condiciones de carga elevada el rendimiento disminuye drásticamente debido al gran número de colisiones. Si se diseña la red adecuadamente, aislando tráfico en subredes cuando sea necesario, este problema puede solucionarse. Otra de sus grandes ventajas es la sencillez del protocolo, lo cual va a permitir que sea fácilmente integrable en el firmware de las interfaces de red. Posteriormente se buscaron nuevos soportes físicos. Ethernet se llevó sobre cable de cobre de par trenzado sin apantallar (UTP). Este entorno se conoce como 10BaseT. El elemento que permitió llevar el protocolo CSMA/CD sobre par trenzado fue el concentrador 10BaseT. Este elemento tiene varias entradas para par trenzado, a cada una de las cuales se conecta el cable de par trenzado que viene de una estación, formando una estrella físicamente. Internamente el concentrador ejecuta el protocolo CSMA/CD, detectando las colisiones que se produzcan entre las distintas entradas de par trenzado. También se llevó sobre fibra óptica. El método seguido es similar al caso de 10BaseT: la fibra se conecta a un módulo (concentrador) de fibra óptica que internamente detecta la colisiones. Hay dos normas utilizadas actualmente 10BaseFB y FOIRL (enlace entre repetidores por fibra óptica). La ventaja de una respecto a la otra es que 10BaseFB utiliza una conexión síncrona al contrario de FOIRL. Esto permite que los paquetes de datos pasen por más concentradores que los cuatro que constituyen el límite en el caso de FOIRL. La norma FOIRL define los requisitos del transceiver de fibra óptica que se utiliza para enlazar repetidores, cubriendo distancias de hasta un Km. Aunque FOIRL se desarrolló para la conexión de repetidores, a menudo se utiliza para la conexión a Ethernet de dispositivos de usuario cuando se ha elegido fibra óptica como medio de transmisión.

NORMA IEEE 802.5

Esta norma se refiere fundamentalmente a los requisitos de la subcapa de control de acceso al medio, pero se definen también algunas funciones del nivel físico.

El soporte físico que se empezó a utilizar fue el par trenzado apantallado, que se usaba sobre una topología en anillo. Las estaciones se conectaban a unidades MAUs (Multiple Acces Unit). Éstas se conectaban en serie entre ellas y, conectando la primera y la última, se formaba un bucle cerrado o anillo. En la sección siete de la norma se encuentran las especificaciones que definen el par trenzado apantallado, los conectores de interface con el medio y la unidad de acoplamiento troncal que es preciso utilizar en una red Token Ring.

La más conocida de las redes Token Ring propietaria es la de IBM, cuyas normas difieren ligeramente de la 802.5 pero normalmente son compatibles. En realidad la mayoría de los suministradores actuales fabrican sus productos según las normas de IBM. En la actualidad el comité 802.5 se encuentra en proceso de elaboración de nuevas normas que cubran los concentradores activos y pasivos, así como la utilización de UTP y fibra óptica para las conexiones entre estación y concentrador. El protocolo de control de acceso al medio es el paso de testigo en anillo.

El funcionamiento de este protocolo es el siguiente:

Cuando no hay tráfico en el anillo, circula de forma indefinida un testigo de tres octetos. Cuando una estación quiere transmitir debe hacerse con el testigo y, con los dos primeros octetos del testigo, crea la secuencia de inicio de trama. La estación, entonces, manda el resto de la trama normal de datos a la estación destino. Bajo condiciones normales, el primer bit de la trama irá alrededor del anillo y regresará al extremo que transmite, antes de que se haya transmitido la trama completa. En consecuencia, la estación transmisora deberá vaciar el contenido del anillo mientras está transmitiendo, ya que esta función no la realiza la estación destino. El mecanismo de direccionamiento es similar al de Ethernet, cada estación va a poseer una única dirección MAC, implementada en el hardware del interface de red. Una estación puede mantener el testigo durante el tiempo de retención de testigo, que es de 10 ms. Después de haberse transmitido todas las tramas que estaban pendientes, o bien que la transmisión de otra trama llegara a exceder el tiempo de retención del testigo, la estación se encargará de regenerar la trama del testigo de tres octetos y la volverá a colocar sobre el anillo. Token Ring también establece un mecanismo de prioridades. Algunos problemas que pueden surgir con este

protocolo, donde como se puede ver no existen colisiones, son:

− Pérdida del testigo.

− Duplicación del testigo.

− Rotura del anillo.

− Acaparación del anillo por parte de una estación.

− Cada anillo tiene una estación supervisora. En caso de caída de ésta otra estación la sustituye; pero, si la supervisora pierde el control y las demás no detectan su incapacidad, no podrá ser impugnada.

NORMA ANSI X3T9.5

Los usuarios de las redes Ethernet a 10Mbps y Token Ring a 4 o 16 Mbps se encuentran, básicamente con dos problemas:

− Saturación de red, provocada por el aumento de nodos y el uso intensivo de aplicaciones de red (servidores de ficheros, correo electrónico, acceso a bases de datos remotas, etc.).

− Conectividad de las diferentes redes y aplicaciones.

El objetivo de la red FDDI no es sustituir a las redes anteriores; más bien las complementa, intentando solucionar estos problemas. Además se han añadido recursos para la integración de nuevos servicios telemáticos de voz e imagen. La red está estandarizada por el comité X3T9.5 de ANSI (American National Standards Institute). En la norma FDDI se define un nivel físico y un nivel de enlace de datos, usándose fibra óptica como medio de transmisión a una velocidad de 100 Mbps. La norma establece un límite máximo de 500 estaciones, 2 Km entre estaciones y una distancia máxima total de 100 Km FDDI se caracteriza por su topología de doble anillo:

− Un anillo primario: similar al anillo principal de Token Ring.

− Un anillo secundario: similar al anillo de backup de Token Ring.

Cada anillo se forma con un hilo de fibra óptica, por lo que, con un par de hilos de fibra óptica podremos formar el doble anillo FDDI. Según el tipo de conexión al anillo, simple o doble, existen dos tipos de estaciones denominadas SAS (Single−Attached Station) y DAS (Dual−Attached Station) respectivamente. Las primeras necesitan realizar la conexión al anillo mediante un concentrador y, al contrario que las segundas, no forman parte integrante del esquema tolerante a fallos que implementa FDDI. Las estaciones SAS permiten una topología en estrella, característica que las hace adecuadas para su instalación mediante un sistema de cableado PDS como el que se dispone. Para poder llevar a cabo esta última configuración deberíamos tener FDDI sobre cable de cobre UTP, de esto último se encarga TPDDI. La tecnología de FDDI sobre hilo de cobre se inició a principios de 1991. Cabletron desarrolló la tecnología necesaria para transmitir sobre distancias de hasta 100 metros en FDDI con UTP, y hasta 150 metros con STP, sin modificar el esquema actual de codificación FDDI. Actualmente se está a la espera de la aprobación de una norma definitiva.

FDDI se basa en la arquitectura OSI y su especificación se divide en cuatro capas. Las dos primeras se corresponden con el nivel físico, la tercera con el control de acceso al medio y la cuarta abarca a las tres anteriores y realiza funciones de gestión. Las cuatro capas son:

PMD (Physical Media Department). Define la frecuencia y los niveles de los pulsos ópticos que componen la

señal. También especifica la topología y los tipos de fibras y conectores que pueden ser empleados.

PHY (Physical Layer Protocol). Aquí se definen los tipos de codificación (4b/5b) y sincronización.

MAC (Media Acces Control). Comprende los protocolos necesarios para la generación del testigo, la transmisión de la trama y el reconocimiento de direcciones. También se define aquí la estructura o formato de las tramas y el método de corrección de errores. El protocolo de acceso es, básicamente, el mismo que en el caso de Token Ring, aunque con algunas diferencias. La estación que quiere transmitir tiene que esperar a recibir el testigo, una vez en su poder puede transmitir tramas durante un cierto tiempo, transcurrido el cual debe devolver el testigo a la red.

SMT (Station Management). Su misión es la monitorización y gestión de la red. Se divide en tres partes: Frame Services que genera tramas de diagnóstico; CMT (Connection Management), que controla el acceso a la red; y Ring Management que determina los problemas que aparecen en la red física.

SMT monitoriza y gestiona la red mediante una completa lista de funciones que ningún otro protocolo ofrece. Gracias a esto, FDDI es la tecnología de red más sólida y robusta de las que hay actualmente disponibles.

SEGURIDAD EN REDES

INTRODUCCION

El tema de la seguridad de las redes está definitivamente sobre el tapete y requiere soluciones de corto plazo. Cualquier medida de seguridad corporativa, inclusive la incorporación de complejos dispositivos de avanzadas tecnologías, podría ser improductiva si no se enmarca dentro de una estrategia organizacional que establezca las políticas de seguridad, las que deben considerar aspectos tales como autentificación, encriptación, control de acceso físico y lógico, protecciones contra virus y la aplicación de estadísticas y cálculo de probabilidades, si así se requiere, sobre las redes corporativas y, por cierto, al elemento humano que la compone. El acceso no autorizado, daño o mal uso de la información de las empresas se puede traducir en pérdidas financieras inmediatas y, en el mediano plazo, afectar su posición competitiva en el mercado con todos los perjuicios que ello podría significar. Para enfrentar este desafío, la empresa debe establecer sus propias políticas de seguridad, basadas en medidas tecnológicas y administrativas, cimentadas en la identificación de los riesgos, vulnerabilidades e impactos organizacionales a la que se expone a través de sus redes de comunicaciones.

Las redes abiertas, tales como Internet, son hoy en día una herramienta imprescindible para las empresas, sin embargo representan una amenaza constante a su seguridad, por lo que la Conectividad a estas redes requiere una adecuada evaluación de riesgos, de manera de tomar anticipadamente las medidas de seguridad e incorporar los elementos tecnológicos y medidas administrativas necesarias para minimizar los accesos no deseados. Existen innumerables ejemplos que muestran cómo costosos y complejos sistemas y dispositivos de seguridad han sido vulnerados, lo que confirma la tesis que la seguridad debe ser abordada como un todo y en forma integral en la organización. La sola incorporación de dispositivos Corta Fuego (firewall)**,** no garantiza la seguridad de la información, por lo que su implementación debe ser parte de un conjunto de políticas de seguridad organizacional, las cuales son particulares a cada empresa en función de sus necesidades.

La elaboración de una estrategia de seguridad corporativa debe considerar la identificación de amenazas y riesgos, sus vulnerabilidades y el grado de exposición a ellas, una evaluación de los impactos y sus costos organizacionales. Estas tareas requieren del apoyo de expertos independientes.

Firewall

Los Firewalls son barreras creadas entres redes privadas y redes públicas como Internet. Originalmente,

fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. Más recientemente, los sistemas de seguridad proporcionados por terceras empresas, son la solución más escogida.

Los Firewalls son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado. Son diseñados de forma que todo lo que no es expresamente autorizado, es prohibido por defecto.

Un Firewall:

- protege la red interna de una organización, de los usuarios que residen en redes

externas.

− permite el paso entre las dos redes a sólo los paquetes de información autorizados.

- Pueden ser usados internamente, para formar una barrera de seguridad entre diferentes partes de una organización − como por ejemplo a estudiantes y usuarios administrativos de una universidad.

Reflejan un número de decisiones de diseño dependiendo del acceso, seguridad y transparencia.

Es diseñado para entregar un acceso seguro a los servicios ofrecidos por la red Internet con un mínimo esfuerzo adicional. La calidad de este "mínimo esfuerzo" es llamada la "transparencia" que significa que un usuario puede usar un gran número de software comercial sin modificaciones adicionales.

Puede mejorar significativamente el nivel de seguridad en la red y reducir los riesgos filtrando la falta de seguridad inherente en los servicios de Internet.

Implementa una política de acceso a la red, forzando que todas las conexiones a ésta, se realicen a través de él, mientras son examinadas y evaluadas.

Usan Tres Tecnologías Diferentes, son: Filtro de paquetes, Gateways a Nivel de Circuitos y Gateways a Nivel de Aplicación. A veces se usan de forma separada, a veces conjuntamente. El Filtro de Paquetes trabaja a nivel TCP/IP y no tienen control de qué aplicaciones están filtrando. Las Gateways a Nivel de Circuitos interceptan las sesiones y las pasan a través de los Firewall. Las Gateways a Nivel de Aplicación operan al nivel más alto, controlando las aplicaciones que han generado los paquetes.

Filtro de Paquetes

El Filtro de Paquetes trabaja al nivel TCP/IP. Aceptan paquetes pre−aprobados − aquellos que vienen de fuentes particulares o que son direccionados a direcciones específicas de su red. El Filtro de Paquetes es transparente al usuario y puede ser instalado como parte de un Router que entrega la típica conexión a Internet. De todas formas, como solución de seguridad, el Filtro de Paquetes por sí solo, tiene varios fallos. Primero, requieren que el remitente sea pre−aprobado. Usted quizá quiera permitir el acceso a un servicio desde un usuario remoto, pero no a otros servicios. La solución requiere definiciones especiales de qué tipo de servicios pueden ser autorizados. Estas definiciones especiales pueden ser particularmente difíciles de aplicar. Además, se pueden tener problemas con servicios como FTP o DNS. Estas aplicaciones usan protocolos que son extremadamente difíciles de gestionar a nivel de paquetes.

Gateways a Nivel de Circuito

Las Gateways por definición son seguras. Todo el tráfico de entrada y salida está gobernado por una Gateway.

Ya que no hay una conexión física directa entre las máquinas de su red interna y las redes externas, las conexiones de salida pueden ser todavía permitidas cuando el destino sea autorizado.

Las Gateways a Nivel de Circuito usan proxies para asegurar su red interna. Los llamantes establecen conexiones TCP/IP con la Gateway. Una puerta de la Gateway actúa como un agente para sus usuarios. Este agente verifica las transmisiones y las acepta dependiendo del usuario. La Gateway entrega luego los datos a la dirección apropiada de su red interna. Además, la dirección del agente es la única información transmitida externamente en los paquetes de salida. Los Proxies ayudan a limitar la cantidad de información de máquinas individuales que se enseña al mundo exterior. De todas formas, es posible que un usuario interno rompa esta seguridad usando una puerta no estándar o bien un servicio no autorizado.

Al contrario del Filtro de Paquetes, la Gateway a Nivel de Circuito no examina cada paquete de datos. Aceptan múltiples paquetes de datos una vez verificada la información de dirección.

Gateways a Nivel de Aplicación

Las Gateways a Nivel de Aplicación efectúan el mismo tipo de función de las Gateways a Nivel de Circuito con una adición. Examinan los contenidos de cada paquete cuando pasan por la Gateway. Los Hackers no tienen la oportunidad de entrar a su sistema "escondiendo" datos destructivos entre la información aparentemente "sana". Esto es particularmente importante cuando se permite el acceso de correo electrónico externo a su red interna. SMTP no es un protocolo seguro, y es el sistema de vulnerabilidad más común. La Gateway examina tanto los paquetes de salida como de entrada. Esto elimina la posibilidad de que usuarios internos accedan a servicios no autorizados que puedan crear un "agujero" en la seguridad. La Gateway a Nivel de Aplicación es el protocolo de filtro más seguro. Dado que efectúan un detallado análisis de los paquetes, son los más costosos en términos de tiempo y de equipo.

¿Qué debe incluir un Firewall?

Ya decidida que política de seguridad se va a implementar, se necesita evaluar qué servicios se necesitan en un Firewall. Como mínimo, un firewall debe tener las siguientes características y atributos:

Posibilidad de denegar todos los servicios, excepto aquellos específicamente permitidos por el administrador de sistemas

Una administración flexible, para que los nuevos servicios o necesidades se puedan implementar fácilmente Soporte de técnicas líderes de autentificación

El Filtro de IP debe ser flexible, fácil de programar y debe poder filtrar tantos atributos como sea posible, incluyendo dirección IP destino y fuente

Uso de Proxies en servicios como FTP y Telnet

Tener la posibilidad de centralizar el acceso SMTP

Acomodar acceso público al sito

Posibilidad de filtrar y concentrar accesos remotos por llamadas

Contener mecanismos para guardar registros de tráfico y de actividad sospechosa

Generar alarmas para detectar intrusos (el grado debe ser programado por el administrador de sistemas)

Que se ejecute en un host dedicado

Que se base en un sistema operativo seguro

Que sea simple en el diseño por lo que puede ser comprendido y mantenido fácilmente

Que pueda ser actualizado)

NIVELES DE SEGURIDAD

La información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones y además las medidas de seguridad no influyen en la productividad del sistema sino más bien al contrario, por lo que las organizaciones son reacias a dedicar recursos a esta tarea.

Hasta ahora las grandes organizaciones delegaban la seguridad de las comunicaciones a unos departamentos, las copias y archivos de seguridad a otro, la microinformática a otro, el control de acceso a otro y en cada ciudad, región o país con criterios diferentes. Esta situación junto con la explosión de las redes ha llevado a definir la necesidad de incorporar en las organizaciones una persona o un grupo responsable de los sistemas información (DSI) y que no solo debe contemplar aspectos técnicos, ya que la logística, métodos, planificación de recuperación ante desastres, deben configurar el trabajo de este departamento.

A pesar de todo lo que se habla de la seguridad, un reciente estudio indicaba que el para el 25% de los responsables de la información en empresas de más de 100 empleados, a la seguridad no se le da una prioridad alta dentro de la organización y en los casos en que se da esta prioridad, creen que el resto de la organización no da a este tema la atención que requiere.

La seguridad debe contemplar no solo que no acceden intrusos sino que los sistemas y las aplicaciones funcionan y son utilizados correctamente. Los niveles de seguridad no pueden ni deben ser iguales para todos los elementos (usuarios, aplicaciones, etc.) que gestionan la información.

Las medidas de seguridad deben contemplar algunos de los siguientes aspectos:

Identificación biunivoca de los usuarios (Users ID)

Claves de acceso (password) de al menos 6 caracteres y archivos de claves protegidos y encriptados.

Modificación periódica de las claves de acceso (como mínimo cada tres meses)

Registros de control del uso correcto, intentos incorrectos,

Acceso remoto seguro

Cifrado y firma digital en las comunicaciones

Posibilidad de desconectar si no se usa un terminal e identificación de la persona que desconecta.

Salvaguardas y copias de seguridad.

Planificación de desastres.

Formación de los usuarios en los aspectos de seguridad.

El nivel de desarrollo de estas medidas depende de la naturaleza de la organización, de la información, de las aplicaciones, de quienes las usan y acceden a las mismas.

PLAN DE SEGURIDAD

La puesta en marcha de un plan de seguridad no es algo estático que se hace una vez. Una de las principales garantías de que un sistema es seguro es que se realiza un seguimiento de las medidas puestas en marcha, de los registros de auditoria, el seguimiento de las medidas de seguridad es la vía para asegurar que el plan se adapta a la organización y para detectar posibles intentos de fraude o acceso incorrecto.

El desarrollo de redes globales a las que se accede desde cualquier parte del mundo con un costo bajo y desde cualquier hogar como es INTERNET, aumenta estadísticamente la probabilidad de que alguien no autorizado intente acceder a la red.

En un estudio de Datapro Research corp. Se resumía que la distribución de los problemas de seguridad en sistemas basados en redes responde a la siguiente distribución:

Errores de los empleados 50%

Empleados deshonestos 15%

Empleados Descuidados 15%

Intrusos ajenos a la Empresa 10%

Integridad física de instalaciones 10%

Los planes de seguridad deben considerar la tipología de la información, de los usuarios de la misma y de los equipos y sistemas.

En un plan típico de seguridad se deben considerar los siguientes aspectos:

Seguridad física de los locales y acceso donde se encuentran los sistemas.

Asegurarse contra todos los riesgos posibles, esto requiere un periodo de observación y una clasificación de los recursos y sistemas que están en los edificios de la Organización, los que están fuera, los puntos de acceso remoto, las costumbres y hábitos del personal y el uso de la microinformática estática y portátil.

Asegurarse que es una integración por encima de los sistemas, plataformas y elementos que constituyen las redes.

La gestión de la seguridad debe de ser centralizada.

Entrando ya más en el detalle, el plan debe de especificar las tareas a realizar, sus responsables, como se definen los niveles de acceso, como se audita el plan, como se realizara el seguimiento, donde deben de ponerse en marcha medidas especificas (cortafuegos, filtros, control de acceso, etc.), el plan de formación, la estructura organizativa.

El sentido común debe de jugar un papel de relevancia, ya que si no es así, se pueden llegar a proponer medidas muy seguras pero realmente impracticables, lo cual significa que hay que asumir ciertos riesgos.

Amenazas deliberadas a la seguridad de la información

Se entiende por amenaza una condición del entorno del sistema de Información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). Se Puede definir un Ataque o Amenaza como la potencial violación de un sistema de seguridad.

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Estas tácticas o amenazas pueden producirse a partir de alguno de estos hechos:

Modificación ilegal de los programas (virus, Caballos de Troya, borrado de información).

Deducción de Información a partir de datos estadísticos o de uso que se utilizan para reconstruir datos sensibles.

Destrucción y modificación de datos controlada o incontrolada.

Cambiar la secuencia de los mensajes.

Análisis del trafico observando los protocolos y las líneas de comunicación o los discos de los computadores.

Perdida del anonimato o de la confidencialidad.

Uso de una identidad falsa para hacer transacciones o enviar operaciones.

Impedir que a un usuario que puede usar los recursos lo haga.

Violación de los sistemas de control de acceso.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un computador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje Ingresa un millón de pesos en la cuenta A podría ser modificado para decir Ingresa un millón de pesos en la cuenta B.

Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos

Los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes falsos.

Servicios de seguridad

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización.

Estos servicios hacen uso de uno o varios mecanismos de seguridad.

Una clasificación útil de los servicios de seguridad es la siguiente:

Confidencialidad: requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico erróneo al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

Autenticación: requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

Integridad: requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time−stamps.

No repudio: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.

Control de acceso: requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

Disponibilidad: requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

Los "crackers, piratas o violadores informáticos con interés en atacar un sistema para obtener beneficios de forma ilegal, los "hackers" que son aquellos que lo hacen simplemente como pasatiempo y reto técnico (más respetuosos que aquellos con la información) y los "sniffers" que rastrean y observan todos los mensajes que hay en la red, constituyen nuevas tipologías de intrusos que cada vez están adquiriendo mayor relevancia en el panorama de la seguridad.

Los "crackers" una vez que acceden a un sistema pueden entre otras cosas coleccionar las claves de acceso a los diferentes nodos y sistemas de la red para su posterior uso o bien dejar programas que les permiten el posterior acceso al sistema, el objetivo de este es acceder al sistema operativo al más alto grado de prioridad para controlar las aplicaciones, borrar archivos, introducir un virus, Los Agentes externos no constituyen, sin embargo, el mayor peligro para una red área global, un estudio realizado en más de 2000 compañías encontró que el 65% de los gastos incurridos (mas de 5 billones anuales de dólares en perdidas) fueron generados por errores y mal uso de los propios usuarios de la red y no por agentes externos. El ejemplo más claro lo tenemos en los virus informáticos: el 90% de los virus los introducen en las organizaciones los propios usuarios a

través de programas, juegos, disquetes, etc. que nunca deberían de haber usado y que en algún caso tenían prohibido hacerlo.

Mecanismos de seguridad

Los mecanismos para garantizar la seguridad no pueden ser ajenos a los sistemas informáticos que deben de ejecutarlos, de nada sirve poner en un papel que las claves de acceso tendrán 15 caracteres si luego los programas solo admiten 6. Esto que parece tan obvio indica que la gestión de las redes y la seguridad de las mismas son en cierto modo inseparables.

Las password o claves de acceso suelen ser uno de los puntos más vulnerables para atacar un sistema, recordar que cuando se teclea una clave correcta el sistema interpreta que el usuario esta autorizado a hacerlo. En general los usuarios no toman precauciones a la hora de definir sus claves de acceso, se están utilizando algunos programas que generan cadenas que no están en los diccionarios y que son fáciles de recordar para evitar que alguien descubra un montón de claves de una organización sin más que probar con todas las palabras que hay en un diccionario (eso sí, electrónico).

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

Cifrado: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

Integridad de datos: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Firma digital: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

Tráfico de relleno: consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa

si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

Control de encaminamiento: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Unicidad: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.

Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.

Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Planificación de Desastres Los planes de seguridad deben incluir una planificación de desastres de todo tipo (desastres naturales, ataques, sabotajes, etc.).

En estos procedimientos se deben de tener en cuenta los costos que suponen si se legan a producir y los costos en los que hay que incurrir para evitarlos y buscar un compromiso aceptable para la empresa.

Copias de Seguridad Insistimos en que las medidas de seguridad deben de obedecer primero a una regla: sentido común, por ejemplo si solo hay una persona que conoce como hacer y recuperar las copias de seguridad en una organización, esta claro que si ese señor tiene un accidente simultáneamente con un error en el sistema puede ser una tragedia.

El tener procedimientos documentados (y actualizados), evitar los puntos únicos críticos (aquellos que si se paran se para todo el sistema) y siguiendo con este razonamiento el hacer copias de seguridad parece que son medidas de sentido común.

Las copias de seguridad se manejan y gestionan mucho mejor en un sistema centralizado que si se deja esta responsabilidad a los diferentes departamentos.

Señalar algunos aspectos importantes relativos al archivo y las copias de seguridad: Los sistemas de backup para las redes cada vez incorporan más funciones software independientes del hardware sobre el que se hacen las copias. Es muy importante automatizar los procesos evitando siempre que sea posible la intervención manual. Los nuevos estándares permiten operar las funciones de archivo y backup sobre distintas redes y plataformas. El archivo del tipo jerárquico HSM que permite a los usuarios trabajar con archivos que están archivados en una librería o en un sistema off−line y que vacían de los discos duros locales aquellos archivos

que menos se utilizan merecen especial atención si esta pensando en incorporar un nuevo software de backup.

En general es más económico pensar en un sistema de backup centralizado que uno distribuido. Se están imponiendo las librerías o juke−boxes que suministran elevadas capacidades de almacenamiento (100 − 1000 Gigas).

Medidas Antivirus La instalación de un programa Antivirus es la medida más empleada por las Empresas para protegerse de esta "plaga" consiguiendo estabilizar las perdidas que estos infringían a las empresas. Los Antivirus pueden ser preventivos o detectores.

La mayor parte de los virus son una combinación de las siguientes formas de actuar:

Añaden código al final de un programa ejecutable.

Insertan código en el interior de un programa ejecutable.

Emplean técnicas de redirección.

Sobreescribir archivos.

Rodear las funciones y comandos de código creando una verdadera "shell" manejada por el virus.

Bloqueo de las funciones de consulta de directorio, presentando en pantalla una información que no se corresponde con los verdaderos tamaños y fechas del sistema, enmascarando la existencia del virus.

Algunas reglas de sentido común permiten evitar riesgos innecesarios. Por otro lado, recordar de nuevo que la mayor parte de los virus son introducidos en las empresas por los propios empleados. Utilizar PC aislados para probar el software que viene de fuera, utilizar siempre disquetes protegidos contra escritura, hacer backups de forma regular, no cargar software de ocio en los computadores de la empresa.

La seguridad se ve comprometida frente a los ataques de los virus por estas actividades:

Compartir disquetes con programas entre usuarios.

Utilizar programas precompilados

Dejar disquetes sin protección de escritura en los drivers.

Uso de software pirata o software que se obtiene directamente de las redes como Internet.

Permitir el acceso a los computadores a personal no autorizado.

Es importante comprender que un virus se introduce en una red a través de cualquier puerto que permite leer programas o que permite leer archivos que luego se pueden renombrar como programas. El numero de puestos que hay en las redes hacen que éstas sean especialmente vulnerables y además es imposible monitorizar la actividad de todos y cada uno de los usuarios que acceden a esas redes.

Existe un estudio realizado por la división de seguridad del National Institute of Standards and Technology que es una guía para seleccionar herramientas y técnicas de protección contra los virus, que puede serle de utilidad para profundizar en este campo.

Control de acceso: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o

a la red, como por ejemplo mediante las contraseñas de acceso.

El Control de Acceso es uno de los caballos de batalla más importantes en la cadena de la seguridad. El Control de Acceso se puede realizar con sistemas que combinan hardware y software. Una opción utilizada habitualmente son sistemas (módem, software, etc.) que generan una llamada a un puesto o teléfono de control preprogramado, que devuelve al punto de acceso la ID a comprobar. Estos dispositivos se suelen localizar en los centros de gestión de red o en los computadores centrales.

Los controles de Auditoria en los cuales se registra la actividad en general y todas las entradas y salidas que se realizan. Es importante que los sistemas permitan desconectar a los usuarios por inactividad para evitar que alguien se encuentre un computador ya conectado y con todos los derechos activos.

Los sistemas más sofisticados incluyen lectores de tarjetas de crédito, tarjetas inteligentes, detectores de huella digital o simplemente generadores de clave que son únicas para cada sesión.

Cortafuegos Los cortafuegos o "firewalls" son mecanismos que permiten filtrar los accesos permitiendo aislar en función de diferentes criterios o parámetros, quien puede y quien no puede entrar en un sistema. La técnica de cortafuegos es casi de uso obligatorio si sus redes de área local están accesibles a través de Internet.

Los cortafuegos se pueden instalar en los routers, en los servidores o en máquinas aisladas cuya única función es analizar y filtrar lo que puede y no puede acceder de dentro afuera y viceversa.

Las técnicas que se utilizan son una combinación de las siguientes:

Filtrado de paquetes, se especifican que direcciones o PI pueden salir y/o entrar en la red.

Filtrado a nivel aplicativo, que puede controlar parámetros específicos para cada aplicación del servidor, como las horas de llamada, el numero de sesiones, los Identificativos del que llama y del llamado, tipo de servicios requeridos.

CONCLUSIONES

Asegurar la información en una red global debe ser un objetivo ineludible para las organizaciones. Hasta el día de hoy, los sistemas abiertos con poco nivel de control preceden a los mecanismos de seguridad a favor de la integridad y de la confidencialidad de la información. La solución a este problema no es resolver solo un aspecto puntual o una parte del sistema, hay que abordar el conjunto de la red.

La criptografía empieza a ser una pieza vital en la protección de la información ya que permite protegerse de aquellos que solo miran lo que pasa y que por otro lado son los más difíciles de detectar. Por otro lado como cada vez es más difícil saber por que caminos y sistemas va a pasar la información, la criptografía asegura la confidencialidad de la información allá donde este. El inconveniente es la sobrecarga de los computadores y la falta de un estándar que sea aceptado globalmente.

Es evidente que la comunidad de la aldea global deberá de llegar a un compromiso que garantice la confidencialidad, pero que en determinados casos permita la intervención, para evitar que el uso de las autopistas de la información se convierta en una vía segura de comunicación para narcotraficantes, terroristas, ya que si no es así, este mismo motivo se convertirá en razones de estado suficientes para paralizar el desarrollo de esta nueva vía de comercio, cultura y desarrollo que no sabe de fronteras.

Las medidas de seguridad no solo son de tipo técnico, deben de ser aceptadas y entendidas por todos y cada uno de las personas de una organización. Recuerde que el 80% de los problemas de seguridad se generan

dentro de la propia organización.

Los planes de seguridad no son algo estático y exigen su revisión continua y la supervisión como medio de detectar posibles ataques.

No se debe descuidar las medidas de seguridad clásicas que conciernen a cosas tan bien entendidas como los virus, las copias de seguridad, el control y gestión de correctas claves de acceso.

Si se utiliza Internet es obligatorio desarrollar una política adaptada a sus necesidades y al nivel de conexión y servicios que se quiera dar. Asegure que los procedimientos se utilizan, supervisando regularmente el buen y adecuado uso de las políticas que se decidan.

La Seguridad debe de constituir, la prioridad máxima si se esta decidido a hacer negocio en Internet. Los riesgos son altos y deben de tomarse en serio, a veces pensamos que esas cosas solo pasan en América, pero la realidad es que en Internet desaparecen las fronteras.