35

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

ANALISIS Y MONITOREO DE REDES DE COMPUTADORAS PARA ACCESO VIA INTERNET

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A N:

CONSTANTINO GUTIERREZ SANJUAN

LILIANA KARINA OROPEZA HUERTA

RAYMUNDO GAYTAN PEREZ

VIRGEN ADRIANA POLANCO ORTIZ

DIRECTOR DE TESIS:

ING. NORMA ELVA CHAVEZ RODRIGUEZ

MEXICO, D. F. MAYO 2002

AGRADECIMIENTOS

A nuestra Máxima Casa de Estudios:

Por abrirnos las puertas a un mundo de conocimientos.

A nuestra Facultad:

Por brindarnos la oportunidad de formarnos como Ingenieros

A todos nuestros Profesores:

Que compartieron sus conocimientos y nos guiaron
para cumplir esta meta tan anhelada.

A la Ing. Norma Elva Chávez:

Por su ayuda en la elaboración de este trabajo de tesis.

ANÁLISIS Y MONITOREO DE REDES DE COMPUTADORAS PARA ACCESO VÍA INTERNET

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

En una etapa caracterizada por grandes avances tecnológicos, donde los negocios se efectúan a grandes velocidades, gracias a la disponibilidad de infraestructura del comercio electrónico, se vuelve fundamental el racionalizar y optimizar el uso de los recursos y por lo mismo, de las inversiones de una Empresa.

La información constituye un insumo vital y crítico en el mundo de los negocios, las finanzas, el derecho, el entorno académico y todo sin dejar de lado la cultura, las artes y las ciencias en general.

En tan sólo unos años las redes de computadoras han pasado de ser algo oculto, sólo conocido y utilizado por unos pocos a ocupar un primer plano en cualquier medio informativo de carácter general. Quizá el protagonismo que actualmente se da a términos como "Internet", "autopistas de la información" o "aldea global" sea más fruto de las modas que de una necesidad real, pero no cabe duda que dichos términos (o al menos las ideas que representan) tendrán un interés creciente en los años venideros y permanecerán con nosotros durante bastante tiempo.

Podemos hacer un cierto paralelismo entre la explosión de la Telemática en la década de los noventa y el auge de la Informática personal en los ochenta; sin embargo a pesar de su importancia la aparición de la PC no parece comparable a la revolución que está protagonizando la Telemática; la razón estriba en que, a pesar de todo, la PC aislada es hasta cierto punto un producto minoritario, mientras que el sistema multimedia de los noventa conectado a las redes se convierte en una fuente de información y entretenimiento de interés para el público en general.

Los precios de la informatica vienen sufriendo desde hace bastantes años una disminución exponencial. El precio del espacio en disco se reduce a la mitad aproximadamente cada 4.5 años, el de la potencia del procesador cada 2.3 años, y el de la memoria RAM cada 1.8 años. Como comparación el precio de la transmisión de datos se reduce a la mitad cada 1.5 años aproximadamente, es decir; esta teniendo una disminución aún mayor que las tecnologías informáticas. Las investigaciones y desarrollos en materia de transmisión de datos hacen prever que dicha tendencia se mantendrá en el futuro.

Además de los factores tecnológicos en los precios de los servicios telemáticos influyen aspectos legales que en ocasiones alteran la situación de manera importante. Por ejemplo en España, como en otros países de Europa, la decisión de liberalizar las telecomunicaciones en 1998 está produciendo un abaratamiento de los precios gracias a la libre competencia, que de forma transitoria hará aún mayor la reducción que cabría esperar de los factores puramente tecnológicos.

Prácticamente cualquier empresa que tenga varias computadoras hoy en día tiene una red local que los inter-conecta. Si la empresa dispone de varias sedes u oficinas dispersas dispondrá típicamente de una red local[1] (LAN, Local Area Network) en cada una de ellas y de

[1] Se analizará con más detalle en el capítulo 2.3 "Redes de Transmisión"

aplicaciones se conoce como CSCW (Computer Supported Cooperative Work) y también como "groupware".

Hasta aquí hemos discutido aplicaciones orientadas fundamentalmente al uso de la red dentro de la propia empresa (lo que actualmente se suele denominar la "Intranet"[3]).

Dicha red puede conectarse al exterior, bien directamente o a través de un firewall[4], es decir, un gateway intermedio que permita controlar el acceso (entrante y/o saliente) para evitar problemas de seguridad. Cuando la red de la empresa se conecta al exterior (normalmente a la Internet) aparecen una serie de nuevas aplicaciones que le dan aún mayor utilidad.

Algunos ven a Internet como el medio de un nuevo modelo de ventas; algo similar a lo que sucedió cuando aparecieron los centros comerciales o al giro que más tarde introdujeron los grandes almacenes por departamentos. Pero la Red es mucho más que eso. Internet va a revolucionar, o está revolucionando, de forma más profunda que cualquier otro suceso, la operación de las empresas de todos los sectores. Internet es la base de un nuevo orden empresarial.

En las actividades de marketing; por ejemplo, se puede poner el catálogo de productos de la empresa en la red para su consulta por los clientes, con información detallada de características, precio, referencias, etc.; también es posible tramitar pedidos recibidos a través de la red.

Actividades de soporte en línea; se puede responder a preguntas de los usuarios a través de la red, tanto por correo electrónico como por listas de distribución o grupos de news. En el caso de empresas de software es frecuente ofrecer a través de la red nuevas versiones de programas, sistemas operativos, parches para la resolución de problemas, etc.

Las herramientas de comunicación antes mencionadas (correo electrónico, videoconferencia, etc.) adquieren una relevancia mucho mayor cuando su uso no se limita al interior de la empresa.

Algunas empresas encuentran en Internet una manera económica de interconectar sus oficinas remotas, evitando así la contratación de líneas propias de larga distancia.

El empleado puede acceder a una enorme cantidad de información externa a su empresa útil para su trabajo, por ejemplo información de suministradores, competidores, clientes, foros de discusión sobre temas relacionados con su trabajo, etc.

El acceso a información actualmente se centra en el acceso a Internet y sobre todo a servidores Web. En torno a esto han aparecido multitud de servicios derivados del uso de la Telemática para diversos fines, tales como tele-trabajo, tele-compra, tele-enseñanza, tele-medicina, etc.

[3] Red interna
[4] Se verá en el capítulo IV "Monitoreo de redes en aplicaciones vía Internet"

La comunicación tiene lugar tanto en el ámbito individual (correo electrónico) como en grupos (listas de distribución, grupos de news, etc.). Esto incluye no sólo información textual, sino también multimedia: sonido, imagen y vídeo.

Ante este panorama, se vuelve necesario mantener la red en las mejores condiciones, por lo tanto el Monitoreo de Redes es una de las actividades fundamentales de la administración de Redes ya que éste facilita la entrada de datos cuya finalidad es proporcionar la información necesaria para efectuar un correcto análisis y a su vez contribuir con el proceso de toma de decisiones sobre cuando crecer la infraestructura actual, cuando cambiar de tecnología, etc. Sus tareas comprenden entre otras cosas, la extracción e interpretación de datos relacionados con el estado, respuesta y el desempeño de los dispositivos conectados a la red. Mediante su correcta interpretación y llevando un registro histórico de los acontecimientos que van sucediendo, el administrador de la red podrá determinar de manera más rápida el comportamiento de los componentes asociados a la infraestructura e incluso adelantarse y predecir el deterioro del nivel de servicio en alguna parte de la red o en su totalidad.

El propósito de este trabajo, es presentar un estudio de los elementos más importantes a monitorear en una red, relacionados con el desempeño de los recursos de infraestructura, basándose en herramientas automatizadas existentes en el mercado, capaces de ser adecuadas a procesos sistemáticos que ayuden a una correcta interpretación de datos que contribuya con información útil para detectar y prevenir problemas en la red.

Sobre la base de estándares de la Industria los proveedores de tecnología y el mercado empresarial, sea cual sea el tamaño de éste, buscan y adquieren soluciones más rápidas y servicios que apoyen sus estrategias de productividad y competitividad, soportado por el uso inteligente de los servicios de Internet ya sea para una parte específica del negocio o para su totalidad. Ahora Internet ofrece la alternativa ideal para que un negocio se propague eliminando barreras geográficas, ofreciendo la posibilidad de comunicarse con proveedores de todo el mundo o bien en sus propias sucursales logrando así eficientar los procesos de comunicación para mejorar condiciones de operación del negocio y así obtener mayores ganancias.

El desarrollo de esta tesis está orientado a empresas medianas y grandes cuya capacidad económica les permite invertir en Sistemas de Monitoreo, cabe mencionar que se hará referencia a Software al que puede acceder cualquier tipo de usuario.

Se basará en el análisis de los conceptos básicos para el diseño de una red, se estudiará la influencia de estos en el desempeño de la funcionalidad y seguridad de la misma y se mencionarán algunos programas más comúnmente utilizados que realizan mediciones como: el porcentaje de utilización de la red, fallas en los dispositivos, distribución de protocolos, analizadores de estado, elaboración de reportes y bitácoras, disparadores de alertas, etc.

CAPÍTULO I

ANTECEDENTES HISTÓRICOS

CAPITULO I

ANTECEDENTES HISTORICOS

1.1 Antecedentes históricos de las redes de computadoras

Hoy en día, las computadoras están presentes en todas las áreas de la actividad humana. En el hogar, en la oficina, en los bancos, en las agencias de viajes, en los hoteles, en las escuelas y universidades, en la industria, en las fábricas, en los almacenes, etc. Una sola computadora resulta valiosa por su capacidad para procesar información sin necesidad de influencia externa, sin embargo consideremos las capacidades adicionales que dispondría si se conectara a otras computadoras y desplegara la información de ellas. La puerta se abriría hacia un mundo mucho mayor de información. Una red hace posible esto y mucho más.

Las redes constan de dos o más computadoras conectadas entre sí y permiten compartir recursos e información. La información suele consistir en archivos y datos, los recursos son los dispositivos o áreas de almacenamiento de datos compartidos mediante la red. Para comprender lo que son las redes, es importante conocer la manera en que han evolucionado hasta llegar a lo que son en la actualidad.

Comenzaremos nuestro bosquejo histórico en 1969 con el estándar RS-232C que fue creado específicamente para indicar el método para conectar el equipo de datos (la terminal ante la que se sienta el usuario) al equipo para comunicación de datos(el modem conectado a las líneas telefónicas). En la actualidad se usa para conectar todo tipo de dispositivos a las computadoras, incluyendo modems, mouses, impresoras en serie y hasta otras computadoras. El estándar RS-232C se aplica para bajas velocidades de transmisión (menos de 38Kbps) y cortas distancias(hasta 30m). Ver Fig.1.1

Fig 1.1

En los años 70's surge el estándar de transmisión síncrona para incrementar la tasa y la longitud de transmisión de un enlace. Este estándar se conoce como SDLC (Synchronous Data Link Control) y su principal idea es evitar el consumo de tiempo en la transmisión y para ello agrupa los bits de información en paquetes (packets). Ver fig. 1.2 Dos computadoras entonces ya pueden compartir información.

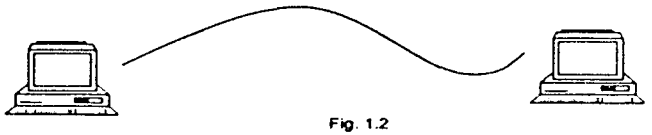


Fig. 1.2

El primer documento que estudia la idea de conmutación por paquetes de los que se tiene conocimiento fue un estudio realizado por las Fuerzas Aéreas de los Estados Unidos de Norteamérica. Durante el periodo de 1962 a 1964, la agencia ARPA del Departamento de Defensa de Estados Unidos de Norteamérica, fomentó la investigación de sistemas de tiempo compartido resultando la red ARPANET que entró en operación en 1969, con cuatro nodos. Este nuevo estándar permite conectar fácilmente una red y hoy en dia se usa para conectar un gran número de computadoras en el mundo tal como una Red de Área Local (LANs).

A finales de 1960 y principios de 1970, se propuso un nuevo método de enlace, este método es llamado *acceso* múltiple que reduce el costo de conexión. En la fig. 1.3 se muestra una red de acceso múltiple llamado Ethernet en la cual las computadoras se comunican a través de una interfaz integrada a cada una de ellas y por medio de cable coaxial.

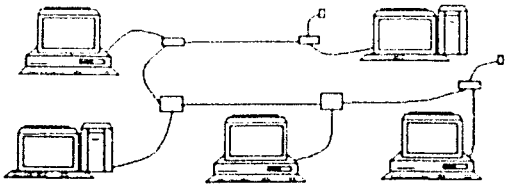


Fig 1.3

Poco después ARPA dio a conocer un proyecto llamado internetting, cuyo principal objetivo era conectar diferentes redes, pero para su funcionamiento era necesario un moderador para realizar la comunicación. En 1974 se hizo la primera propuesta de un protocolo de comunicación que controlaba los paquetes de información a transmitir llamado TCP/IP[1] (Transmission Control Protocol/ Internet Protocol) que fue integrado al proyecto ARPA para tener un sistema operativo orientado a redes de comunicaciones terrestres.

[1] Se analizará en el capítulo 3.5 "Protocolos TCP/IP"

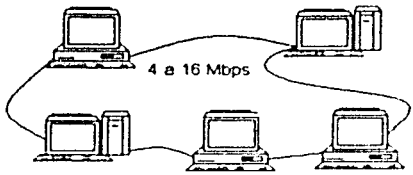


Fig. 1.4

A principios de 1980, IBM desarrolla otro método de acceso múltiple llamado Token Ring, que se muestra en la fig.1.4. Así las computadoras tienen un enlace de punto a punto uni-direccional usando una tarjeta de interfaz Token Ring. Pero la transmisión de información tanto en la red Token Ring como en una red Ethernet seguía siendo demasiado lenta para algunas aplicaciones multimedia. Por lo que tiempo después se desarrolla una nueva red llamada Fiber Distributed Data Interface (FDDI) mostrado en la fig.1.5. La red FDDI utiliza fibra óptica para transmitir a 100 Mbps y puede ofrecer servicios para aplicaciones que combinen audio, video y datos integrados.

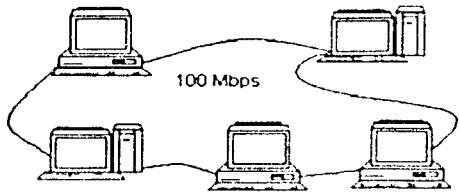


Fig 1.5

En 1986 se crea el estándar Synchronous Optical Network (SONET) con el objetivo de unificar la interconexión de redes de los sistemas Estadounidense, Europeo y Japonés.

Luego en 1988 se estableció el estándar para circuitos virtuales conocido como "Frame" denominada Frame Relay, ofreciendo una velocidad de 2 Mbps.

A comienzos de 1991 empezaron a surgir nuevas tecnologías de redes de alta velocidad, una de ellas el ATM (Asynchronous Transfer Mode) la cual transmite información a una velocidad de entre 25 Mbps a 2 Gbps en paquetes de 53 bytes llamados cells, ver fig. 1.6. Actualmente el estándar SONET es utilizado por una gran variedad de proveedores de servicio para transporte FDDI, ATM, incluyendo sistemas punto apunto y en anillo.

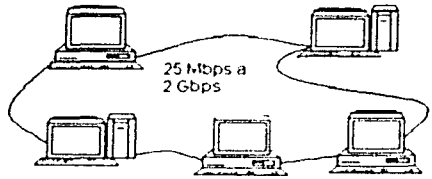


Fig 1.6

En 1992 se estableció una sociedad internacional llamada ISOC para promover el conocimiento de Internet y su tecnología, la cual pudo difundir audio y video en vivo en forma digital por todo el mundo.

A partir de 1994 se empieza a aplicar la tecnología Fast Ethernet a 100 Mbps, principalmente para aplicaciones multimedia y acceso a Intranet. Posteriormente en 1997 esta velocidad es superada hasta llegar a 1 Gbps, utilizado para archivos de imagen y manejo de bases de datos.

En 1999 surge un nuevo Internet (Internet 2) desarrollada por varias universidades de Estados Unidos en la que es posible tener un canal de comunicación de hasta 665 Mbps. Actualmente esta tecnología proporciona mejores aplicaciones y servicios a los usuarios de Internet como son; comercio electrónico, video-conferencias, información, correo electrónico, entre otros.

1.2 Internet

Internet nace a fines de la década de los 60's, como un proyecto del Departamento de Defensa de los Estados Unidos para diseñar un sistema de comunicaciones distribuido. El proposito de esta red era posibilitar las comunicaciones entre las autoridades en caso de un ataque nuclear. Las redes de comunicaciones de ese tiempo estaban diseñadas de modo que cada nodo de la red dependía del nodo anterior. Si se destruía un nodo toda la red sería inutilizada. A partir de esto, se diseño una pequeña red descentralizada que conectaba computadoras en cuatro universidades en Estados Unidos, estructurada conceptualmente como lo que hoy entendemos como red.

Como mencionamos antes a esta se le se llamo ARPANET y uno de sus objetivos fue compartir los recursos de las supercomputadoras entre los investigadores universitarios. Pronto esta red se convierte en una oficina postal de alta velocidad, al convertirse el correo electrónico en el medio de comunicación preferido en estas universidades, con el objeto de compartir y colaborar en proyectos de investigación.

En 1971 ARPANET se extiende a 23 sitios (hosts o máquinas) conectando a los centros de investigación de universidades y de gobierno en los Estados Unidos. En 1973 ARPANET se internacionaliza al conectar dos centros en Inglaterra y en Noruega.

Alrededor de 1975 el proyecto es un éxito por lo que su administración pasa al Departamento de Comunicaciones de Defensa de Norteamérica. Hacia 1981, ARPANET tenía 213 nodos y creciendo a un ritmo de un nodo cada 20 días. A mediados de los 80s se crea el protocolo TCP/IP que permite tener un lenguaje común para todas las computadoras conectadas que en 1983 fueron adoptados por ARPANET.

ARPANET estaba compuesto por cientos de computadoras pertenecientes a universidades, centros de investigación militar y algunas compañías, conectadas entre sí. El servicio más popular entonces, era el correo electrónico que permitía una fácil y rápida comunicación entre diferentes personas conectadas a ARPANET. El sistema operativo que más se usaba era UNIX y en especial una versión de UNIX desarrollada por la universidad de California en Berkeley llamada BSD UNIX.

Entonces se comienza a visualizar esta colección de redes como una gran red: Interworking, que finalmente se abrevia Internet. En esta misma época, IBM introdujo las computadoras personales y comenzo la revolucion de la computación personal. Al mismo tiempo se introdujeron las computadoras poderosas listas para redes (como Sun) que permitieron que muchas compañías ingresaran a Internet y se comunicaran entre sí.

Para 1985 las redes locales en computadoras personales ya estaban progresando y esto ayudó a completar la idea de Internet. Ya se podía tener redes, subredes, y conectar redes de área ancha (WAN) con redes locales (LAN). En 1986 surge un programa de supercomputadoras iniciado por Fundación Nacional de Ciencia (NSF), el propósito de este programa era hacer que los recursos de super cómputo puedan llegar a cualquier usuario. Ellos establecieron 5 centros de super cómputo en diferentes áreas de Estados Unidos y construyeron una red que los uniera a todos. La NSF basó sus protocolos de comunicacion en los protocolos de Internet y se originó lo que se conoció como NSFNET que fue el corazon de Internet hasta 1995. Para entonces se utilizaba el e-mail, FTP, Telnet y otros servicios de Internet.

En 1989 un equipo de investigación en Suiza perteneciente al Centro Europeo de Investigación de Partículas, desarrollo una serie de protocolos para transferir hipertexto via Internet. A principios de 1990, un grupo de personas pertenecientes al National Center For Supercomputing Application (NCSA) mejoraron esos nuevos protocolos y desarrollaron el NCSA Mosaic, el primer navegador que hacia el uso de Internet algo fácil. Fue entonces cuando comenzó el boom del World Wide Web que atrajo a miles de personas hacia Internet.

Internet ha cambiado nuestra forma de percibir las cosas. Como se puede ver, la comunidad que se desarrolla en Internet no es nueva, y aunque antes era dominada principalmente por investigadores y universidades, ahora se está adentrando poco a poco en nuestra vida diaria. Personas de diferentes países tienen un medio de comunicacion accesible y rápida. Barreras ideológicas se rompen y se mezclan. Cuando antes existía una falta de información, ahora tenemos una sobredosis de la misma: Universidades, bibliotecas, museos, libros, etc. todos en línea. Internet ha desarrollado una cultura propia, basado en una sociedad virtual compuesta por personas de todas partes del mundo

La gran rapidez con la que Internet se ha expandido y popularizado en los últimos años ha supuesto una revolución muy importante en el mundo de las comunicaciones llegando ha causar cambios en muchos aspectos de la sociedad.

CAPÍTULO II

REDES DE COMPUTADORAS

CAPITULO II

REDES DE COMPUTADORAS

2.1 Descripción de red de comunicación

Se puede pensar por un momento en el servicio de correos. Cuando alguien desea mandar una carta a otra persona, la escribe, la mete en un sobre con el formato impuesto por correos, le pone un sello y la introduce en un buzón; la carta es recogida por el cartero, clasificada por el personal de correos, según su destino y enviada a través de medios de transporte hacia la ciudad destino; una vez allí otro cartero irá a llevarla a la dirección indicada en el sobre; si la dirección no existe, al cabo del tiempo la carta regresará al origen por los mismos cauces que llegó al supuesto destino.

Más o menos, esta es la forma en que funciona una red: la carta escrita es la información que se quiere transmitir; el sobre y sello es el paquete con el formato impuesto por el protocolo que se utiliza en la transmisión; la dirección del destinatario es la dirección del nodo destino y la dirección del remitente, será la dirección del nodo origen, los medios de transporte que llevan la carta cerca del destino es el medio de transmisión (cable coaxial, fibra óptica); las normas del servicio de correos, carteros y demás personal son los protocolos de comunicaciones establecidos.

La expresión "redes de computadoras" (o simplemente redes) se utiliza cuando, por medio de la Telemática, se realiza la comunicación entre dos o más computadoras. Queda excluida aquí la comunicación entre una computadora y un periférico (terminal, impresora, etc.) independientemente de la distancia a la que dicha comunicación se produzca o el tipo de medios utilizados para ella. Dicho de otro modo, en redes de computadoras se considera únicamente la comunicación entre elementos que pueden hablar de igual a igual ("peer to peer" en inglés), sin tomar en consideración la comunicación asimétrica maestro-esclavo.

Un caso particular de las redes de computadoras son los sistemas distribuidos, en los que se intenta conectar varias computadoras mediante una red y crear un entorno de utilización tal que el usuario no perciba la existencia de múltiples sistemas, sino que los maneje como un único sistema virtual de forma transparente; para esto se utilizan normalmente protocolos[1] o aplicaciones específicas. Evidentemente si el medio de comunicación es de baja velocidad el usuario percibirá un retraso cuando acceda a un nodo remoto, por lo que generalmente los sistemas distribuidos solo se implementan en redes de alta velocidad (redes locales por ejemplo). Un ejemplo de protocolo de sistemas distribuidos podría ser el NFS (Network File System) que permite acceso a archivos remotos de forma transparente.

Cuando se envían datos por un canal de transmisión analógico (por ejemplo una línea telefónica de RTB) es preciso modular la señal en origen y demodularla en el destino; el aparato

[1] Se definirá en el capítulo 3.2 "Protocolos"

que realiza esta función se llama modem. Inversamente, cuando enviamos una señal analógica por un canal de transmisión digital tenemos que codificarla en origen y decodificarla en destino, para lo cual se utiliza un aparato denominado codec; por ejemplo un teléfono RDSI es un codec, ya que convierte una señal analógica (la voz humana) en digital, y viceversa; un sistema de videoconferencia es un codec puesto que convierte una señal analógica (la imagen en movimiento captada por la cámara) en una señal digital (la transmitida por RDSI u otro medio); también hay un codec en cualquier sistema de grabación digital de sonido (CD, Minidisc, DCC, DAT). Es frecuente referirse a los codecs como conversores analógico-digital o conversores A/D, aunque en telecomunicaciones suele preferirse la denominación codec.

Para desempeñar su labor un codec debe hacer un muestreo periódicamente la onda a digitalizar, y convertir su amplitud en una magnitud numérica. Por ejemplo los sistemas de grabación digital del sonido en CD hacen un muestreo de la señal de cada canal de audio 44 100 veces por segundo (44.1 KHz) y generan para cada muestra un número entero de 16 bits que representa la amplitud de la onda. En la decodificación se realiza el proceso inverso.

Los bits se transmiten por un canal realizando modificaciones en la onda portadora; por ejemplo en una línea telefónica podemos utilizar una frecuencia de 1 KHz para representar el 0 y una de 2 KHz para el 1; esto se conoce como modulación de frecuencia; si sincronizamos dos equipos para que transmitan un cambio de frecuencia de la portadora cada 3.333 milisegundos podremos transmitir datos a 300 bps, (si, dos bits consecutivos son iguales en realidad no hay tal cambio). Si en vez de dos frecuencias utilizamos cuatro, por ejemplo 0.5, 1, 1.5 y 2 KHz, podremos transmitir con la misma sincronización 600 bps, ya que enviamos dos bits cada vez al disponer de cuatro estados o niveles posibles; análogamente si utilizamos ocho estados podremos transmitir 900 bps (tres bits por vez), y así sucesivamente; ganamos en velocidad, pero a cambio tenemos que ser más precisos en la frecuencia ya que el número de valores permitidos es mayor. Al número de cambios de estado o sincronizaciones por segundo que tienen lugar en una comunicación entre dos equipos se le denomina baudios; así en nuestro ejemplo anterior todas las transmisiones se hacían a 300 baudios, aunque el número de bits que se transmitía por segundo era diferente en cada caso. Además de la frecuencia es posible modular la amplitud y la fase de la onda portadora; en la práctica los modems modernos modulan una compleja combinación de las tres magnitudes para extraer el máximo provecho posible de las líneas telefónicas, es decir el máximo número de bps a un número de baudios dado.

A pesar de todo el ingenio utilizado, los canales de transmisión tienen un límite. Ya en 1924 Nyquist observó la existencia de un límite fundamental en las transmisiones digitales sobre canales analógicos, que se conoce como teorema de Nyquist, y que establece que el número máximo de baudios que puede transmitirse por un canal no puede ser superior al doble de su ancho de banda. Así, en el caso de la transmisión de datos por una línea telefónica, con un ancho de banda de 3 KHz, el máximo número de baudios que puede transmitirse es de 6,000.

Se puede comprender intuitivamente el teorema de Nyquist si se imagina cual sería la frecuencia que tendría una señal digital que transmitiera 6 Kbaudios; supongamos por sencillez que 1 baudio = 1 bps, o sea que manejamos únicamente dos estados, y que utilizamos una corriente de 1 voltio para indicar un bit a 1 y de -1 voltio para indicar un bit a 0; la frecuencia

mínima de la señal, que sería de cero hertzios, se produciría cuando transmitiéramos continuamente ceros o unos, mientras que la frecuencia máxima se produciría cuando transmitiéramos la secuencia 010101..., momento en el que obtendríamos una onda cuadrada de 3 KHz de frecuencia (ya que cada dos bits forman una oscilación completa); así pues para transmitir 6 Kbaudios necesitaríamos un ancho de banda de 3 KHz, conclusión que coincide con la que habríamos obtenido a partir del teorema de Nyquist.

El teorema de Nyquist no establece el número de bits por baudio, que depende del número de estados que se utilicen. Así en el caso anterior si en vez de dos valores de voltaje utilizamos cuatro (-2, -1, 1 y 2 voltios por ejemplo) con el mismo número de baudios (y de hertzios) podemos duplicar el número de bits por segundo.

Podemos expresar el teorema de Nyquist también en forma de ecuación relacionándolo con la velocidad máxima de transmisión, así si H es el ancho de banda y V el número de niveles o estados posibles, entonces la velocidad máxima de transmisión C viene dada por:

$$C = 2\,H \log_2 V$$

Por ejemplo, un canal telefónico (H= 3 KHz) con tres bits por baudio (ocho estados, V=8) la máxima velocidad de transmisión posible es 18 Kbps.

Podemos calcular también la eficiencia de un canal de comunicación, E, que es la relación entre la velocidad de transmisión y el ancho de banda:

$$E = C/H$$

Así en nuestro ejemplo anterior la eficiencia era de 6 bits/Hz.
Combinando las dos fórmulas anteriores podemos expresar de otra forma el Teorema de Nyquist:

$$E = 2 \log_2 V$$

Dicho de otro modo, la eficiencia máxima de un canal está fijada por el número de estados diferentes de la señal, o sea por la forma como se codifica ésta.

Debido a la relación directa que el teorema de Nyquist postula entre ancho de banda y velocidad de transmisión es frecuente en Telemática considerar ambas expresiones como sinónimos; así decimos por ejemplo que la transmisión de grandes archivos necesita un elevado ancho de banda queriendo decir que requiere una elevada velocidad de transmisión.

El teorema de Nyquist es bidireccional, es decir, también se aplica en el sentido opuesto, cuando se trata de una conversión analógico-->digital. Por ejemplo, para que un teléfono RDSI (codec) pueda capturar la señal de audio sin mermar la calidad respecto a una línea analógica, el teorema de Nyquist establece que la frecuencia de muestreo deberá ser como mínimo de 6 KHz. En la práctica los teléfonos digitales hacen un muestreo a 8 KHz para disponer de un cierto margen de seguridad. Los sistemas de grabación digital de alta fidelidad, que hacen un

muestreo a 44.1 KHz, son capaces de capturar sonidos de hasta 22 KHz lo cual excede la capacidad del oído humano (en la práctica suelen filtrarse todas las frecuencias superiores a 20 KHz).

Cuando el teorema de Nyquist se aplica en este sentido se le suele denominar teorema de muestreo de Nyquist.

Ley de Shannon-Hartley

El teorema de Nyquist supone la utilización de un canal de comunicación perfecto, es decir sin ruido. En la realidad los canales tienen, aparte de otros tipos de ruido, un ruido aleatorio llamado también ruido térmico, que se mide por su valor relativo a la señal principal, y se conoce como relación señal-ruido, S/R o S/N (signal-noise ratio). El valor de esta magnitud se suele indicar en decibelios (dB), que equivalen a 10 log10 S/N (así 10 dB equivalen a una relación S/R de 10, 20 dB a una relación de 100 y 30 dB a una de 1000). Dado que la percepción de la intensidad del sonido por el oído humano sigue una escala logarítmica la medida en decibelios da una idea más exacta de la impresión que producirá un nivel de ruido determinado (este parámetro es uno de los que se utilizan para medir la calidad de los componentes de un equipo de reproducción musical de alta fidelidad). En 1948 Shannon y Hartley generalizaron el teorema de Nyquist al caso de un canal de comunicación con ruido aleatorio, derivando lo que se conoce como la ley de Shannon-Hartley, que está expresada en la siguiente ecuación:

$$C = H \log2 (1 + S/N)$$

(De nuevo aquí H representa el ancho de banda y C la velocidad de transmisión). Por ejemplo, con un ancho de banda de 3 KHz y una relación señal-ruido de 30 dB (o sea 1000, valor típico de una buena conexión telefónica) obtenemos una velocidad de transmisión máxima de 29 902 bps. Si la relación señal-ruido desciende a 20 dB (cosa bastante normal) la velocidad máxima baja a 19 963 bps.
Si lo expresamos en términos de eficiencia obtendremos:

$$E = \log2 (1 + S/N)$$

Vista de este modo la Ley de Shannon-Hartley establece una eficiencia máxima para un valor dado de la relación señal-ruido, independientemente de la frecuencia y del ancho de banda asignado al canal. Así por ejemplo, para una relación señal-ruido de 40 dB la eficiencia máxima teónca es de 13.3 Bps/Hz.

Elementos de una Red

Los principales elementos que necesitamos para instalar una red son:

- Tarjetas de interfaz de red
- Cable

- Protocolos de comunicaciones.[2]
- Sistema operativo de red.
- Aplicaciones capaces de funcionar en red.

Tarjetas de interfaz de red

Las tarjetas de interfaz de red (NICs - Network Interface Cards) son adaptadores instalados en un dispositivo, cuya función es conectarlo en red. Es el pilar que sustenta toda red local, y el único elemento imprescindible para enlazar dos computadoras a buena velocidad (excepción hecha del cable y el software). Existen tarjetas para distintos tipos de redes. Las principales características de una tarjeta de red son:

- Operan a nivel físico del modelo OSI[3]: Las normas que rigen las tarjetas determinan sus características, y su circuitería gestiona muchas de las funciones de la comunicación en red como:

  Especificaciones mecánicas: Tipos de conectores para el cable, por ejemplo.

  Especificaciones eléctricas: definen los métodos de transmisión de la información y las señales de control para dicha transferencia.

- Método de acceso al medio: es el tipo de algoritmo que se utiliza para acceder al cable que sostiene la red. Estos métodos estan definidos por las normas 802.x del IEEE[4].
- La circuitería de la tarjeta de red determina, antes del comienzo de la transmisión de los datos, elementos como velocidad de transmisión, tamaño del paquete, time-out, tamaño de los buffers. Una vez que estos elementos se han establecido, empieza la verdadera transmisión, realizándose una conversión de datos a transmitir a dos niveles:

  1.- En primer lugar se pasa de paralelo a serie para transmitirlos como flujo de bits.

  2.- Seguidamente se codifican y a veces se comprimen para un mejor rendimiento en la transmisión

- La dirección física es un concepto asociado a la tarjeta de red: Cada nodo de una red tiene una dirección asignada que depende de los protocolos de comunicaciones que esté utilizando. La dirección física habitualmente viene definida de fábrica, por lo que no se puede modificar. Sobre esta dirección física se definen otras direcciones, como puede ser la dirección IP para redes que estén funcionando con TCP/IP[5].

---

[2] Se analizará en el capítulo 3.2. "Protocolos"
[3] Se analizará en el capítulo 3.4. "Modelo OSI"
[4] Para más detalle ver capítulo 3.1 "Estándares"
[5] Para más detalle revisar capítulo 3.5 "Protocolos TCP/IP"

Determinación de la velocidad de transmisión en una red

Existen varios factores que determinan la velocidad de transmisión de una red, entre ellos podemos destacar:

- El cable utilizado para la conexión. Dentro del cable existen factores como:

  El ancho de banda permitido.
  La longitud.

- Las tarjetas de red.
- El tamaño del bus de datos de las máquinas.
- La cantidad de retransmisiones que se pueden hacer.

Medios de transmisión

El medio de transmisión, es probablemente la parte más crítica en el diseño de una red, especialmente cuando se trata de redes locales. Mientras que el conjunto de protocolos a utilizar suele estar determinado de antemano por factores externos, y permite por tanto poco margen de maniobra, en el medio físico de transmisión se dan generalmente varias posibilidades razonables.

Además las inversiones que se hacen en infraestructura suelen ser la parte más importante de la red y la más difícil de modificar más adelante. Por otro lado, este es un campo que por suerte o desgracia evoluciona con mucha rapidez, y lo que hoy puede parecer adecuado quizá no lo sea dentro de dos años; para tomar una decisión acertada es necesario hacer una estimación objetiva de las necesidades actuales y futuras, y una valoración adecuada de las tecnologías disponibles tomando en cuenta su relación costo/beneficio.

Los medios de transmisión utilizados actualmente son:

Pares de cobre

Este es el medio de transmisión más común, consistente en un par de hilos de cobre aislados, de alrededor de 1 milímetro de diámetro. Un cable suele llevar varios hilos (típicamente 4 u 8) que normalmente están doblados dos a dos formando una doble (o cuádruple) hélice, como una molécula de ADN, por lo que se le suele denominar cable de pares trenzados (twisted pair). Esto se hace para minimizar la interferencia eléctrica que pueden recibir de fuentes próximas, como por ejemplo los pares vecinos, y la que pueden emitir al exterior. Los cables pueden o no estar aislados.

El ancho de banda depende de múltiples factores: el grosor del cable, la distancia, el tipo de aislamiento, la densidad de vueltas o grado de trenzado, etc. Pueden llegar a transmitir con capacidades del orden de Mbps a varios kilómetros.

Existen varios tipos de cables de pares trenzados que difieren fundamentalmente en la frecuencia máxima a la que pueden trabajar, que a su vez viene determinada principalmente por la densidad de vueltas y por el tipo de material aislante que recubre los pares. Estos tipos se conocen como categorías y son las siguientes:

Categoría	Frecuencia máxima (MHz)	Usos	Vueltas/metro
1	No se especifica	Telefonía, datos a corta distancia y baja velocidad	0
2	1	LANs de baja velocidad (1 Mbps)	0
3	16	LANs hasta 10 Mbps	10-16
4	20	LANs hasta 16 Mbps	16-26
5	100	LANs hasta 100 Mbps, ATM a 155 Mbps	26-33
5e	250	LANs hasta 100 Mbps, ATM a 155 Mbps	
6	350	LANs hasta 100 Mbps, ATM a 155 Mbps	

Características principales de los cables según su categoría

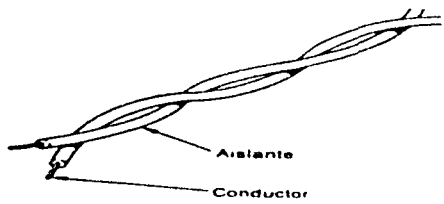


Fig 2.1 Cable de par trenzado

Cable coaxial

El cable coaxial es otro medio de transmisión común. Tiene mejor aislamiento que el par trenzado de cualquier tipo y categoría, por lo que puede llegar a distancias y velocidades mayores.

Un cable coaxial esta formado por un núcleo de cobre rodeado de un material aislante; el aislante está cubierto por una pantalla de material conductor, que según el tipo de cable y su calidad puede estar formada por una o dos mallas de cobre, un papel de aluminio, o ambos. Este material de pantalla está recubierto a su vez por otra capa de material aislante.

Por su construcción el cable coaxial tiene una alta inmunidad frente al ruido, y puede llegar a tener unos anchos de banda considerables. En distancias de hasta 1 Km. es factible llegar a velocidades de 1 ó 2 Gbps. El cable coaxial debe manipularse con cuidado ya que por ejemplo un golpe o doblez excesivo pueden producir una deformación en la malla que reduzca el alcance del cable.

La nomenclatura de los cables Ethernet tiene 3 partes:

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros de segmento multiplicados por 100.

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos : máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mb/seg. Segmentos : máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos : máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg.
100-BASE-X	Fast Ethernet Velocidad de transmisión: 100 Mb/seg.

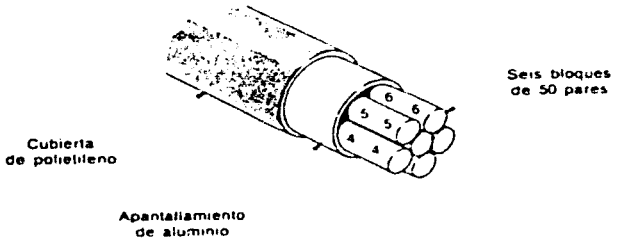


Figura Estructura típica de un cable de pares

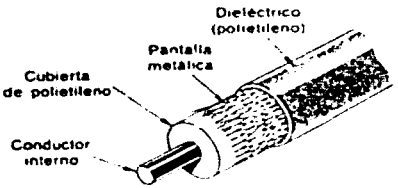


Fig 2.2 Estructura típica de un cable coaxial

Fibra óptica

Si hubiera que mencionar un único factor como el principal causante del elevado desarrollo que han tenido las comunicaciones telemáticas en los años recientes, ese factor sería sin duda la fibra óptica.

Recordemos que tanto el teorema de Nyquist como la ley de Shannon-Hartley establecen que la capacidad de un canal viene limitada por su ancho de banda, que a su vez esta limitada por la frecuencia de la señal portadora. Así pues, si queremos aumentar la capacidad deberemos

subir la frecuencia portadora; siguiendo por este camino llegamos a la luz visible. Sólo necesitamos tres elementos: un emisor, un medio de transmisión, y un detector.

Existen básicamente dos sistemas de transmisión de datos por fibras ópticas: los que utilizan LEDs (Light-Emitting Diode) y los que utilizan diodos láser. En los sistemas que utilizan LEDs la transmisión de un pulso de luz (equivalente a un bit) genera múltiples rayos de luz, pues se trata de luz normal no coherente; se dice que cada uno de estos rayos tiene un modo y a la fibra que se utiliza para transmitir luz de emisores LED se la denomina fibra multimodo. Las fibras se especifican indicando el diámetro de la fibra interior y exterior; las fibras multimodo típicas son de 50/100 y 62.5/125 micras (que significa diámetro interior de 62.5 y exterior de 125 micras); a título comparativo, un cabello humano tiene un diámetro de 80 a 100 micras.

Los diodos láser emiten luz coherente, hay un único rayo y la fibra se comporta como un guía-ondas; la luz se propaga a través de ella sin dispersión; la fibra utilizada para luz láser se llama fibra monomodo. Las fibras monomodo se utilizan para transmitir a grandes velocidades y/o a grandes distancias. La fibra interior (la que transmite la luz) en una fibra monomodo es de un diámetro muy pequeño, de 8 a 10 micras (del mismo orden de magnitud que la longitud de onda de la luz que transmite); una fibra monomodo típica es la de 8.1/125 micras.

Para aprovechar las fibras ópticas de largo alcance actualmente se utilizan varias longitudes de onda por fibra en cada una de estas ventanas, mediante lo que se conoce como multiplexación por división en longitud de onda de banda ancha (wideband WDM, Wavelength Division Multiplexing). Se espera que la WDM en banda estrecha permita extraer aún más capacidad de una sola fibra, pudiendo llegar a compartir una misma fibra varias empresas portadoras, cada una con uno o varios haces transportando la información a diferentes frecuencias.

Cuando se transmite un pulso por una fibra multimodo los rayos se reflejan múltiples veces antes de llegar a su destino, con ángulos diversos (todos por encima del ángulo límite, pues de lo contrario se perderían) lo cual hace que la longitud del trayecto seguido por los rayos que forman el pulso no sea exactamente igual para todos ellos; esto produce un ensanchamiento del pulso recibido, conocido como dispersión.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz ($c = 3 \times 10^8$ m/s), mientras que las señales eléctricas recorren los cables a una velocidad entre el 50 y el 80 por ciento de ésta, según el tipo de cable.

- Mayor capacidad de transmisión. Pueden lograrse velocidades por encima de 1 Gbit/s.

- Inmunidad total ante interferencias electromagnéticas. La fibra óptica no produce ningún tipo de interferencia electromagnética y no se ve afectada por rayos o por pulsos electromagnéticos nucleares (NEMP) que acompañan a las explosiones nucleares.

- No existen problemas de retorno de tierra, crosstalk o reflexiones como ocurre en las líneas de transmisión eléctricas.

- La atenuación aumenta con la distancia más lentamente que en el caso de los cables eléctricos, lo que permite mayores distancias entre repetidores.

- Se consiguen tasas de error típicas del orden de 1 en 10^9 frente a las tasas del orden de 1 en 10^6 que alcanzan los cables coaxiales. Esto permite aumentar la velocidad eficaz de transmisión de datos, reduciendo el número de retransmisiones y corregir los errores de transmisión.

- No existe riesgo de cortocircuito o daños de origen eléctrico.

- Los cables de fibra óptica pesan la décima parte que los cables de corte apantallados. Esta es una consideración de importancia en barcos y aviones.

- Los cables de fibra óptica son generalmente de menor diámetro, más flexibles y más fáciles de instalar que los cables eléctricos.

- Los cables de fibra optica son apropiados para utilizar en una amplia gama de temperaturas.

- Es más difícil realizar escuchas sobre cables de fibra óptica que sobre cables eléctricos. Es necesario cortar la fibra para detectar los datos transmitidos. Las escuchas sobre fibra óptica pueden detectarse fácilmente utilizando un reflectometro en el dominio del tiempo o midiendo las pérdidas de señal.

- Se puede incrementar la capacidad de transmisión de datos añadiendo nuevos canales que utilicen longitudes de onda distintas de las ya empleadas.

- La fibra óptica presenta una mayor resistencia a los ambientes y liquidos corrosivos que los cables eléctricos.

- Las materias primas para fabricar vidrio son abundantes y se espera que los costos se reduzcan a un nivel similar al de los cables metálicos.

- La vida media operacional y el tiempo medio entre fallos de un cable de fibra optica son superiores a los de un cable electrico.

- Los costos de instalacion y mantenimiento para grandes y medias distancias son menores que los que se derivan de las instalaciones de cables eléctricos.

- La mayor desventaja es que no se puede perforar fácilmente este cable para conectar un nuevo nodo a la red.

- Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación, que consiste en una pérdida de amplitud o intensidad de la señal, lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros.

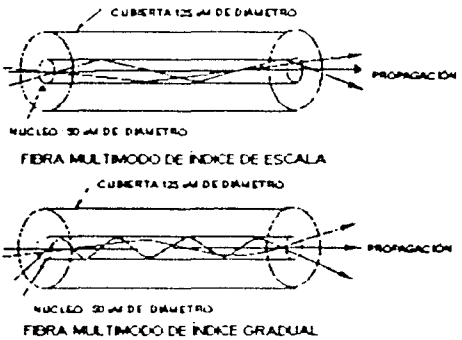


Fig 2.3 Propagación multimodo en una fibra óptica de índice de escala y de índice gradual

Medios inalámbricos enlaces ópticos al aire libre

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire.

Fig 2.4

El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la línea de vista. Las aplicaciones típicas para estos enlaces se

encuentran en los campus de las universidades, donde las carreteras no permiten tender cables, o entre los edificios de una compañía en una ciudad en la que resulte caro utilizar los cables telefónicos.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Lo beneficios de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos.

Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s .

El límite para comunicaciones fiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Existen dos efectos atmosféricos importantes a tener en cuenta con los enlaces ópticos al aire libre:

- La dispersión de la luz que atenúa la señal óptica en proporción al número y al tamaño de las partículas en suspensión en la atmósfera. Las partículas pequeñas, como la niebla, polvo o humo, tienen un efecto que es función de su densidad y de la relación existente entre su tamaño y de la longitud de onda de la radiación infrarroja utilizada. La niebla, con una elevada densidad de partículas, de 1 a 10 μm de diámetro, tienen un efecto más intenso sobre el haz de luz. Las partículas de humo, más grandes, tienen menor densidad y, por tanto, menor efecto.

- Las brisas ascensionales (originadas por movimientos del aire como consecuencia de las variaciones en la temperatura) provocan variaciones en la densidad del aire y, por tanto, variaciones en el índice de refracción a lo largo del haz. Esto da lugar a la dispersión de parte de la luz a lo largo del haz. Este efecto puede reducirse elevando el haz de luz lo bastante con respecto a cualquier superficie caliente o utilizando emisores múltiples. La luz de cada emisor se ve afectada de diferente forma por las brisas, y los haces se promedian en el receptor.

Estos sistemas suelen emplearse para transmisiones digitales de alta velocidad en banda base. En EE.UU., todos los fabricantes de productos láser deben tener una certificación que garantiza la seguridad de sus productos.

Microondas

Los enlaces de microondas se utilizan mucho como enlaces allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda

de SHF[6], de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.

Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2, 4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionara hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo.

Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores.

Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

Luz infrarroja

Permite la transmisión de información a velocidades muy altas: 10 Mbits/seg. Consiste en la emisión/recepción de un haz de luz; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

Señales de radio

Consiste en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesaria la visión directa de emisor y receptor.

La velocidad de transmisión suele ser baja: 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Comunicaciones vía satélite

Los satélites artificiales han revolucionado las comunicaciones desde los últimos 20 años. Actualmente son muchos los satelites de comunicaciones que están alrededor de la tierra dando servicio a numerosas empresas, gobiernos y entidades.

Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite a un satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o

[6] Frecuencia Super Alta (Super High Frecuency)

imágenes de televisión. De esta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencia diferentes.

La capacidad que posee un satélite de recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los gigahertz.

La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36000 Km. sobre el ecuador. Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

Ventajas y Desventajas

Existe un retardo de unos 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento en ocho de un satélite geoestacionario necesitan transmisiones frecuentes de tramas de sincronización.

Los satélites tienen una vida media de 7 a 10 años, pero pueden sufrir fallos que provocan su salida de servicio. Es, por tanto, necesario disponer de un medio alternativo de servicio en caso de cualquier eventualidad.

Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad. Las estaciones situadas en la banda de bajas frecuencias (la banda C) están dotadas de grandes antenas (de unos 30 metros de diámetro) y son extremadamente sensibles a las interferencias. Por este motivo suelen estar situadas lejos de áreas habitadas. Las estaciones que trabajan en la banda Ku disponen de una antena menor y son menos sensibles a las interferencias. Utilizar un enlace de microondas de alta capacidad sólo ayudaría a complicar los problemas de ruido que presente el enlace con el satélite.

Las comunicaciones con el satelite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estacion. Es necesario utilizar técnicas de encriptación[1] para garantizar la privacidad de los datos.

Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol en el que la tierra se sitúa entre el Sol y el satelite, se corta el suministro de energía a las células solares que alimentan el satelite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción o pérdida de servicio.

[1] Para mayor detalle revisar capítulo IV "Monitoreo de redes"

En el caso de tránsitos solares, el satélite pasa directamente entre el Sol y la Tierra provocando un aumento del ruido térmico en la estación terrena, y una pérdida probable de la señal enviada por el satélite.

Los satélites geoestacionarios no son totalmente estacionarios con respecto a la órbita de la tierra. Las desviaciones de la órbita ecuatorial hacen que el satelite describa una figura parecida a un ocho, de dimensiones proporcionales a la inclinación de la órbita con respecto al ecuador. Estas variaciones en la órbita son corregidas desde una estación de control.

Actualmente hay un problema de ocupación de la órbita geoestacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados (anteriormente era de 4). Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda en forma de ruido.

2.2 Topologías de conexión

La topología de una red define únicamente la distribución del cable que interconecta las diferentes computadoras, es decir, es el mapa de distribución del cable que forma la Intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El costo que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una Intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

Topología Física

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topologías físicas puras:

- Topología en anillo.
- Topología en bus.
- Topología en estrella.

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por más de una topología física.

Topología lógica

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

- Topología anillo-estrella: implementa un anillo a través de una estrella física.
- Topología bus-estrella: implementa una topología en bus a través de una estrella física.

Topología Física

Topología en bus

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cual es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

Como ejemplo más conocido de esta topología, encontramos la red Ethernet de Xerox. El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

Consta de un único cable que se extiende de una computadora a la siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada terminador, que además de indicar que no existen más computadoras en el extremo, permiten cerrar el bus.

Sus principales ventajas son:

- Fácil de instalar y mantener.

- No existen elementos centrales de los que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

Sus principales inconvenientes son:

- Si se rompe el cable en algún punto, la red queda inoperable por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unirlas todas a través de un bus troncal.

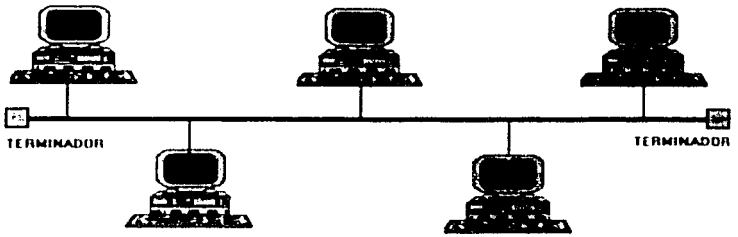


Fig 2.6 Topología en forma de bus

Topología en anillo

Los nodos de la red se disponen en un anillo cerrado conectados a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella. El anillo es fácilmente expandido para conectar mas nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

Sus principales características son:

- El cable forma un bucle.
- Todas las computadoras que forman parte de la red se conectan a ese anillo.

- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo "paso de testigo", es decir sólo observan la información pasar.

Los principales inconvenientes serían:

- Es difícil de instalar.
- Requiere mantenimiento.

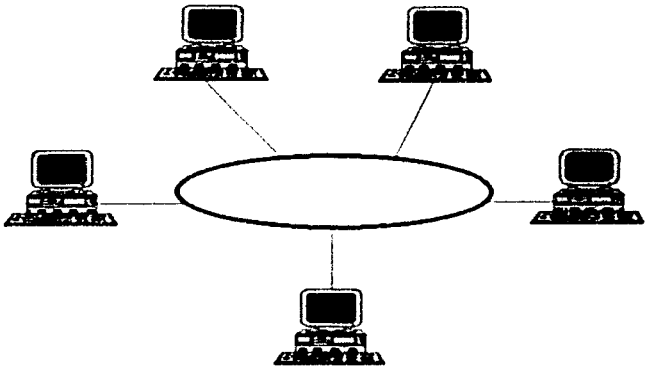


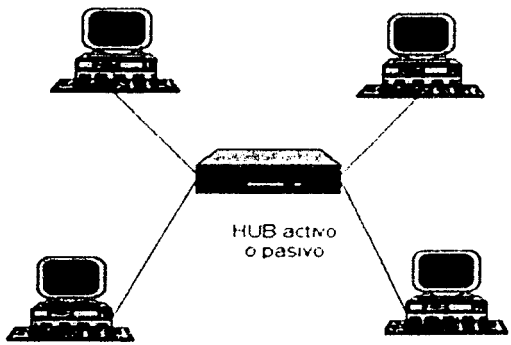
Fig 2.7 Topología en anillo

Topología en Estrella

Sus principales características son:

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.
- Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio poolling, siendo el nodo central el que se encarga de implementarlo
- Cada vez que se quiere establecer comunicación entre dos computadoras, la información transferida de uno hacia el otro debe pasar por el punto central.
- Existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.

- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
- Este tipo de topología se utiliza cuando la transmisión de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
- Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
- Es fácil de detectar y de localizar un problema en la red.



2.8 Topología en estrella pasiva

Estrella Pasiva

Se trata de una estrella en la que el punto central al que van conectados todos los nodos es un concentrador (hub) pasivo, es decir, se trata únicamente de un dispositivo con muchos puertos de entrada.

Estrella Activa

Se trata de una topología en estrella que utiliza como punto central un hub activo o bien una computadora que hace las veces de servidor de red. En este caso, el hub activo se encarga de repetir y regenerar la señal transferida e incluso puede estar preparado para realizar estadísticas del rendimiento de la red. Cuando se utiliza una computadora como nodo central,

es éste el encargado de gestionar la red, y en este caso suele ser además del servidor de red, el servidor de archivos.

TOPOLOGÍAS LÓGICAS

Topología anillo-estrella

Uno de los inconvenientes de la topología en anillo era que si el cable se rompía toda la red quedaba inoperativa; con la topología mixta anillo-estrella, éste y otros problemas quedan resueltos. Las principales características son:

- Cuando se instala una configuración en anillo, el anillo se establece de forma lógica únicamente, ya que de forma física se utiliza una configuración en estrella.
- Se utiliza un concentrador, o incluso un servidor de red (uno de los nodos de la red, aunque esto es el menor número de ocasiones) como dispositivo central, de esta forma, si se rompe algún cable sólo queda inoperativo el nodo que conectaba, y los demás pueden seguir funcionando.
- El concentrador utilizado cuando se está utilizando esta topología se denomina MAU (Unidad de Acceso Multiestación), que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.
- A simple vista, la red parece una estrella, aunque internamente funciona como un anillo.
- Cuando la MAU detecta que un nodo se ha desconectado (por haberse roto el cable, por ejemplo), puentea su entrada y su salida para así cerrar el anillo.

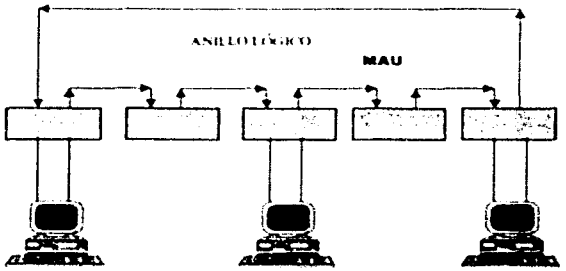


Fig 2.9 Topología anillo-estrella

Topología bus-estrella

Este tipo de topología es en realidad una estrella que funciona como si fuese en bus. Como punto central tiene un concentrador pasivo (hub) que implementa internamente el bus, y al que están conectadas todas las computadoras. La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

Interconexión de redes

Hace algunos años era impredecible la evolución que las comunicaciones, en el mundo de la informática, iban a tener, no podían prever que fuese necesaria la interconexión ya no sólo de varias computadoras sino de cientos de ellas. No basta con tener las computadoras en una sala conectadas, es necesario conectarlas a su vez con las computadoras del resto de las salas de una empresa, y con el resto de las sucursales de una empresa situadas en distintos puntos geográficos.

La interconexión de redes permite, si se puede decir así, ampliar el tamaño de una Intranet. Sin embargo el término interconexión se utiliza para unir redes independientes, no para ampliar el tamaño de una.

El número de computadoras que componen una Intranet es limitado, depende de la topología elegida, (recuérdese que en la topología se define el cable a utilizar) aunque si lo único que se quisiera fuera sobrepasar el número de computadoras conectadas, podría pensarse en simplemente segmentar la Intranet. Sin embargo existen otros factores a tener en cuenta.

Cuando se elige la topología que va a tener una Intranet se tienen en cuenta factores, como son la densidad de tráfico que ésta debe soportar de manera habitual, el tipo de aplicaciones que van a instalarse sobre ella, la forma de trabajo que debe gestionar, etc., esto debe hacer pensar en que, uno de los motivos por el que se crean diferentes topologías es por tanto el uso que se le va a dar a la Intranet. De aquí se puede deducir que en una misma empresa puede hacerse necesaria no la instalación de una única Intranet, aunque sea segmentada, sino la implantación de redes independientes, con topologías diferentes e incluso arquitecturas diferentes y que estén interconectadas.

Habitualmente la selección del tipo y los elementos físicos de una Intranet, se ajusta a las necesidades que se tiene; por este motivo pueden encontrarse dentro de un mismo edificio, varias Intranets con diferentes topologías, y con el tiempo puede surgir la necesidad de interconectarlas.

Se puede ver que por diferentes razones se hace necesaria tanto la segmentación como la interconexión de Intranets, y que ambos conceptos a pesar de llevar a un punto en común, parte de necesidades distintas.

La tabla siguiente refleja de forma escueta diferentes casos en los que se plantea la necesidad de segmentar y/o interconectar Intranets, dando la opción más idónea para cada uno de los casos planteados.

NECESIDAD	SOLUCIÓN
Debido a la necesidad de manejo de aplicaciones que producen un tránsito importante de información aumenta el tráfico en la red; esto lleva a que baje el rendimiento de la misma.	Dividir la red actual en varios segmentos: segmentar la red.
Se tiene que ampliar el número de puestos que forman la Intranet, pero se necesita mantener el rendimiento de la red.	Crear un nuevo segmento de red en el que se pondrán los nuevos puestos e incluso al que se pueden mover puestos, que por disposición física pueda ser conveniente que pertenezcan al nuevo segmento creado en la misma.
Se tiene la necesidad de unir dos Intranets exactamente iguales en la empresa.	Se puede optar por definir una de ellas como un segmento de la otra y unirlas de esta forma; o bien, interconectar las dos Intranets con un dispositivo de nivel bajo.
Se tiene la necesidad de unir dos o más redes con diferentes topologías pero trabajando con los mismos protocolos de comunicaciones.	Es necesario la interconexión de ambas redes a través de dispositivos interconectantes de nivel medio.
Se tiene la necesidad de unir dos o más redes totalmente diferentes, es decir, de arquitecturas diferentes.	Es necesaria la interconexión de ambas redes a través de dispositivos interconectantes de nivel alto.

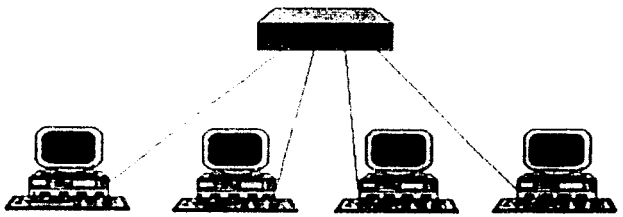


Fig 2.10 Red inicial con topología lógica en bus y física en estrella a través de un Hub

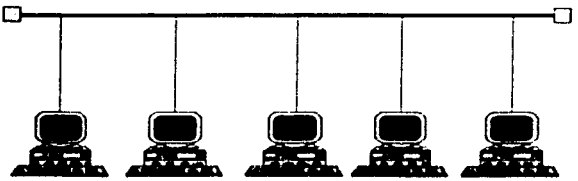


Fig 2.11

Si se necesita ampliar la red, una solución puede ser como la mostrada en la Fig. 2.11, pero no mejora el rendimiento de la red porque lógicamente está vista como una única red.

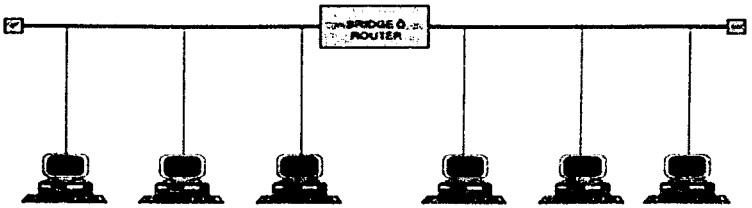


Fig 2.12

Una solución para ampliar la red puede ser la mostrada en la Fig. 2.12 esta topología mejora el rendimiento de la red.

Segmento

Un segmento es un bus lineal al que están conectadas varias estaciones y que termina en los extremos. Las características son:

- Cuando se tiene una red grande se divide en trozos, llamados segmentos a cada uno de ellos.
- Para interconectar varios segmentos se utilizan bridges o routers.
- El rendimiento de una red aumenta al dividirla en segmentos.
- A cada segmento junto a las estaciones a el conectadas se las llama subred.

Segmentación

Segmentar una Intranet consiste en dividirla en subredes para así poder aumentar el número de computadoras conectadas a ella y/o el rendimiento de la misma.

Cuando se segmenta una Intranet, lo que se esta haciendo es crear subredes pequeñas que, por decirlo de alguna manera, se autogestionan, de forma que la comunicación entre segmentos se realiza cuando es necesario, es decir, cuando un nodo de un segmento quiere comunicarse con un nodo del otro segmento; mientras tanto cada segmento de la Intranet está trabajando de forma independiente por lo que en una misma Intranet se están produciendo varias comunicaciones de forma simultánea; evidentemente esto mejora el rendimiento de la Intranet.

La tabla siguiente refleja las longitudes máximas de los segmentos dependiendo de las diferentes topologías de red.

TOPOLOGÍAS	LONGITUD
Ethernet gruesa	500 metros
Ethernet fina	185 metros
Ethernet de par trenzado	100 metros
Ethernet de fibra óptica	2.000 metros
Token-Ring de par trenzado	100 metros

El dispositivo que se utiliza para segmentar una red debe ser inteligente ya que debe ser capaz de decidir hacia qué segmento debe enviar la información llegado a él: si hacia el mismo segmento desde el que la recibió o hacia otro segmento diferente.

Abstrayéndose de algunos detalles, es facil pensar que segmentar una Intranet, ya que se habla de subredes, es como interconectar Intranets diferentes. Sin embargo, cuando se habla de segmentar se hace referencia a una unica Intranet; esto lleva asociado lo siguiente: una única topología, un único tipo de protocolo de comunicaciones, un único entorno de trabajo; cuando se habla de interconectar Intranets, en la mayoria de los casos, las Intranets tienen como mínimo topologías diferentes. No obstante, si debe destacarse que los dispositivos que se utilizan para segmentar redes coinciden con algunos de los dispositivos que son utilizados para interconectar redes diferentes.

Dependiendo del tipo de protocolos que se utilicen en la Intranet segmentada, así como de dispositivos que se utilicen para realizar esta segmentación puede hacerse necesario o no el atribuir a cada segmento una dirección de red diferente. Cuando se trabaja con protocolos TCP/IP[8] esto no es necesario, basta con que cada estación tenga su propia dirección IP, y que no aparezcan dos estaciones con la misma dirección, independientemente de si están o no en el mismo segmento de la Intranet.

[8] Para mayor detalle revisar capítulo 3.5 "Protocolos TCP/IP"

Existen diferentes motivos por los que se puede hacer necesaria la segmentación de una Intranet, como pueden ser:

- Necesidad de sobrepasar el número de nodos que la topología permite. La limitación del numero de nodos en una Intranet vienen impuesta por varios factores, como son el método de acceso al medio que se utiliza, el tipo de cable, el ancho de banda, etc.

- Mejorar el rendimiento de una Intranet en la que ha aumentado el tráfico. En ocasiones, una Intranet que inicialmente funciona bien, con un tiempo de repuesta aceptable, empieza a perder prestaciones; el motivo es claro: de forma paulatina se ha ido incrementando el número de comunicaciones que la Intranet debe gestionar, por diferentes motivos como que los usuarios comienzan a conocer la red y la aprovechan más, o que se han ido instalando más aplicaciones.

Existen diferentes formas de disminuir este problema: Una de ellas, la más drástica es cambiar algún elemento físico de la Intranet: por ejemplo sustituir el cable que implementa la Intranet por uno que pueda soportar velocidades mayores, cambiar las tarjetas de red por otras más rápidas, e incluso cambiar la topología empleada. Una solución menos concluyente consiste en segmentar la Intranet. Dividirla estratégicamente en dos subredes, reduciendo de esta forma el tráfico en cada una de ellas. Por ejemplo, sobre una Intranet inicial repartida por varias aulas de un centro, se pueden crear subredes por aula, de forma que en cada aula se mejorará el rendimiento de la red.

La interconexión de Intranets se puede establecer a varios niveles: desde el nivel físico, a través de un dispositivo llamado hub (concentrador) hasta niveles más altos (niveles del modelo OSI) a través de dispositivos como un puente (Bridge) o un router (encaminador). La tabla siguiente muestra el nivel en el que trabajan los diferentes dispositivos.

DISPOSITIVO	NIVEL
Repetidor	Físico
Concentrador	Físico
Puente	Enlace
Encaminador	Red
Gateway	Aplicación

Para la segmentación de Intranets, y teniendo en cuenta que uno de los motivos por el que se realiza esta operación es mejorar el rendimiento de la red, es necesario emplear dispositivos inteligentes, como pueden ser un encaminador o un puente.

Las redes locales tienen una serie de limitaciones inherentes a su naturaleza:

- Limitaciones en el numero de host
- Limitaciones en la distancia que puede cubrir
- Limitaciones en el número y tipo de nodos que se pueden conectar.

- Limitaciones en el acceso a los nodos.
- Limitaciones en la comunicación con los usuarios.

Para resolver estos problemas se utilizan soluciones de dos naturalezas: software y hardware:

- Elementos de interconexión.
- Software de servicios.

De forma genérica existen varias maneras de ampliar las Intranets:

- Hubs: Para unir hosts dentro de una red.
- Repetidores: conexión a nivel físico, en el mismo segmento.
- Bridges: Conexión a nivel de enlace entre dos segmentos (iguales o distintos).
- Routers: Conexión a nivel de red.
- Gateways: Conexión a nivel de presentación, entre dos redes distintas.

Hubs, Switches, Back bone: Para unir hosts dentro de una red, es un armario de interconexiones, algunas veces el dispositivo realiza funciones de servidor.

Repetidores: conexión a nivel físico, en el mismo segmento, debido a las distancias algunas veces la señal se atenúa por lo que este dispositivo repite la señal para evitar la pérdida o atenuación, al trabajar al nivel mas bajo de la pila de protocolos obliga a que:

- Los dos segmentos que interconecta tenga el mismo acceso al medio y trabajen con los mismos protocolos.
- Los dos segmentos tengan la misma dirección de red.

Fig 2.13

Bridges: Conexión a nivel de enlace entre dos segmentos (iguales o distintos), los protocolos deben ser iguales a partir del nivel de red, se utilizar para ampliar la extensión de red, no importa la topología ni el medio de acceso al medio (pooling o paso de testigo), si son igual únicamente direcciona el paquete, sino realiza traducciones de tramas de una topología a otra, los segmentos tienen direcciones distintas y no trabajan con IP, realizan funciones de reenvio

(filtran, si no corresponden al nodo local lo reenvían), construyen tablas de dirección, trabajan con direcciones físicas.

Routers: Conexión a nivel de red. Un puente avanzado, trabaja con IP, es dependiente del protocolo, conecta LAN y WAN (preferentemente LAN a WAN), eligen rutas eficientes. Cuando llega un paquete al router, éste examina la dirección destino y lo envía hacia allí a través de una ruta predeterminada, si la dirección destino pertenece a una de las redes que el router interconecta, entonces envía el paquete directamente a ella; en otro caso enviará el paquete a otro router más próximo a la dirección destino, para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento. Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos; para ello incorporan un software que pasa un paquete de un protocolo a otro, aunque no son soportados todos los protocolos. Cada segmento de red conectado a través de un router tiene una dirección de red diferente

Gateways. Conexión a nivel capa de aplicación entre redes distintas. Son capaces de traducir información de una aplicación a otra, como por ejemplo los gateways de correo electrónico.

2.3 Redes de Transmisión

De acuerdo con su tecnología de transmisión las redes se clasifican en:

- Redes broadcast (que significa radiodifusión en inglés).
- Redes punto a punto

Según su escala también se suelen clasificar en:

- Redes de área local (LAN, Local Área Network).
- Redes de área extensa (WAN, Wide Área Network)

En esta última clasificación también se distingue a veces una categoría intermedia, la formada por las redes de área metropolitana (MAN, Metropolitan Area Network).

La combinación de estos dos criterios nos permite crear una matriz con cuatro categorías posibles, en la práctica existen redes en cada una de estas cuatro categorías, si bien la mayoría encajan en dos de ellas.

	LAN	WAN
Broadcast	La mayoría de las LANs (Ethernet, FDDI, Token Ring, etc.), Fibre Channel	Redes de transmisión vía satélite
Punto a punto	HIPPI, Fibre Channel, LANs Conmutadas	La mayoría de las WANs (todas las basadas en enlaces telefónicos, X.25, Frame Relay, RDSI, ATM, etc.)

Redes broadcast

En las redes broadcast el medio de transmisión es compartido por todas las computadoras interconectadas. Normalmente cada mensaje transmitido es para un único destinatario, cuya dirección aparece en el mensaje, pero para saberlo cada máquina de la red ha de recibir o "escuchar" cada mensaje, analizar la dirección de destino y averiguar si va o no dirigido a ella; las normas de buena educación "Telemática" establecen que una computadora debe descartar sin mas análisis todo mensaje que no vaya dirigido a él; sin embargo, algunos programas llamados "sniffers"[9] se dedican a "husmear" todo lo que pasa por el cable, independientemente de quien sea su destinatario; con un sniffer es muy fácil capturar cualquier cosa, por ejemplo los caracteres que viajan por la red en un proceso de conexión averiguando así de manera rápida el user-id y la password de un usuario cualquiera (por ejemplo "root"). La única protección efectiva en las redes broadcast es el encriptado de la información[10].

A veces en una red broadcast lo que se quiere es precisamente enviar un mensaje a todas las máquinas conectadas. Esto se llama un envío broadcast. Asimismo es posible enviar un mensaje dirigido a un subconjunto de todas las máquinas de la red (subconjunto que ha de estar definido previamente); esto se conoce como envío multicast (y el subconjunto se denomina grupo multicast). En algunos contextos cuando se habla de broadcast o multicast el caso en el que el mensaje va dirigido a una máquina concreta se denomina envío unicast.

Como ejemplos de redes broadcast se pueden citar casi todas las tecnologías de red local: Ethernet (en sus diversos tipos), Token Ring, FDDI, etc. También son redes broadcast las basadas en transmisión vía satélite. En una red broadcast la capacidad o velocidad de transmisión indica la capacidad agregada de todas las máquinas conectadas a la red; por ejemplo, la red conocida como Ethernet tiene una velocidad de 10 Mbps, lo cual significa que la cantidad máxima de tráfico agregado de todos los equipos conectados no puede superar este valor.

[9] Para mayor detalle ver capítulo IV "Monitoreo de Redes"
[10] Para mayor detalle ver capítulo IV "Monitoreo de Redes"

Redes punto a punto

Las redes punto a punto se construyen por medio de *conexiones* entre pares de computadoras, también llamadas *líneas*, *enlaces*, *circuitos* o *canales* (en inglés los términos equivalentes son "lines", "links", "circuits", "channels" o "trunks"). Una vez un paquete es depositado en la línea el destino es conocido de forma unívoca y no es preciso en principio que lleve la dirección de destino.

Los enlaces que constituyen una red punto a punto pueden ser de tres tipos de acuerdo con el sentido de la transmisión:

- Simplex: la transmisión sólo puede efectuarse en un sentido.
- Semi-dúplex o "half-duplex": la transmisión puede hacerse en ambos sentidos, pero no simultáneamente
- Dúplex o "full-duplex": la transmisión puede efectuarse en ambos sentidos a la vez.

En los enlaces semi-dúplex y dúplex la velocidad de conexión es generalmente la misma en ambos sentidos, en cuyo caso se dice que el enlace es simétrico; en caso contrario se dice que es asimétrico.

La gran mayoría de los enlaces en líneas punto a punto son dúplex simétricos. Así, cuando se habla de un enlace de 64 Kbps sin especificar más se quiere decir 64 Kbps en cada sentido, por lo que la capacidad total del enlace es de 128 Kbps

Al unir múltiples máquinas con líneas punto a punto es posible llegar a formar redes de topologías complejas en las que no sea trivial averiguar cuál es la ruta óptima a seguir para ir de un punto a otro, ya que puede haber múltiples caminos posibles con distinto número de computadoras intermedias, con enlaces de diversas velocidades y distintos grados de ocupación. Como contraste, en una red broadcast el camino a seguir de una máquina a otra es único, no existen computadoras intermedias y el grado de ocupación es el mismo para todas ellas.

Cada una de las computadoras que participa en una red de enlaces punto a punto es un nodo de la red. Si el nodo tiene un único enlace se dice que es un nodo terminal o "end node", de lo contrario se dice que es un nodo intermedio, de encaminamiento o "routing node". Cada nodo intermedio ha de tomar una serie de decisiones respecto a por donde debe dirigir los paquetes que reciba, por lo que también se les llama nodos de conmutación de paquetes, nodos de conmutación, conmutadores o encaminadores (los términos equivalentes en inglés son respectivamente packet switching nodes, switching nodes, switches y routers). Dependiendo del tipo de red que se trate nosotros utilizaremos las denominaciones router o conmutador.

Cualquier computadora (por ejemplo una estación de trabajo UNIX, o incluso una PC con MS/DOS), puede actuar como un router en una red si dispone del programa apropiado; sin embargo, se prefiere normalmente utilizar para este fin computadoras dedicadas, con sistemas operativos en tiempo real y software específico, dejando las computadoras de propósito general para las aplicaciones del usuario, esto da normalmente mayor rendimiento y fiabilidad.

Tradicionalmente a la computadora de propósito general que se conecta a la red como nodo terminal mediante un router se le denomina host, palabra inglesa que significa anfitrión (aunque esta denominación no se utiliza nunca en este contexto). El conjunto de líneas de comunicación y routers que interconectan a los hosts forman lo que se conoce como la subred de comunicaciones, o simplemente subred. Los hosts o nodos terminales no forman parte de la subred.

Para llegar de un nodo a otro en una red se ha de atravesar uno o varios enlaces; el número de enlaces se denomina en inglés "hops", que significa saltos, y depende de la trayectoria seguida y de la topología de la red. Cuando dos nodos no vecinos (es decir a más de un "hop" de distancia) desean intercambiar información lo han de hacer a través de uno o varios nodos intermedios.

Cuando un paquete se envía de un nodo al siguiente normalmente el paquete es transmitido en su totalidad y almacenado; sólo entonces el nodo receptor intenta enviar el paquete al siguiente nodo de la red. Esto es lo que se conoce como una red de almacenamiento - reenvío ("store-and-forward") o red de conmutación de paquetes ("packet - switched"). Esta forma de proceder permite una elevada fiabilidad incluso en entornos hostiles donde el número de errores puede ser elevado.

Dado que en una red punto a punto cada enlace puede tener una velocidad distinta, no podemos caracterizar la red con un único dato de forma tan sencilla como en una red broadcast; sería preciso adjuntar un esquema de la topología indicando el tipo de cada enlace (simplex, semi-dúplex o duplex) y su velocidad (en cada sentido si fuera asimétrico).

Redes de área local (LAN)

Las redes de área local tienen generalmente las siguientes características:

- Tecnología broadcast: medio compartido
- Cableado específico, instalado normalmente a propósito
- Velocidad de 1 a 100 Mbps
- Extensión máxima de unos 3 KM (FDDI llega a 200 Km.)

Las LANs más conocidas y extendidas son la Ethernet a 10 Mbps, la IEEE 802.5 o Token Ring a 4 y 16 Mbps, y la FDDI a 100 Mbps. Estos tres tipos de LAN han permanecido prácticamente sin cambios desde finales de los ochenta, por lo que a menudo se les referencia en la literatura como "LANs tradicionales ("legacy LANs" en inglés) para distinguirlas de otras más modernas aparecidas en los 90´s, tales como la Fast Ethernet (100 Mbps).

A menudo las LANs requieren un tipo de cableado específico (de cobre o de fibra); esto no suele ser un problema ya que al instalarse en una fábrica, campus o similar, se tiene un control completo sobre el entorno y las condiciones de instalación.

El alcance limitado de las LANs permite saber el tiempo máximo que un paquete tardará en llegar de un extremo a otro de la red, lo cual permite aplicar diseños que de otro modo no serían posibles, y simplifica la gestión de la red.

Como consecuencia del alcance limitado y del control en su cableado, las redes locales suelen tener un retardo muy bajo en las transmisiones (decenas de microsegundos) y una tasa de errores muy baja.

La topología básica de las redes locales suele ser de bus (por ejemplo Ethernet) o de anillo (Token Ring o FDDI). Sin embargo, pueden hacerse topologías más complejas utilizando elementos adicionales, tales como repetidores, puentes, conmutadores, etc., como veremos más adelante.

En épocas recientes se ha popularizado una técnica para aumentar el rendimiento de las redes locales, que consiste en dividir una LAN en varias más pequeñas, con lo que el ancho de banda disponible para cada uno es mayor; las diversas LANs así formadas se interconectan en un equipo especial denominado conmutador LAN (o LAN switch); en casos extremos se puede llegar a dedicar una red por equipo, disponiendo así de todo el ancho de banda para él.

En años recientes se ha empezado a utilizar una tecnología de redes telefónicas, y por tanto típicamente de redes WAN, para la construcción de redes locales; esta tecnología, denominada ATM (Asynchronous Transfer Mode), dará mucho que hablar en el futuro.

Redes de área amplia (WAN)

Las redes de amplio alcance se utilizan cuando no es factible tender redes locales, bien porque la distancia no lo permite por el costo de la infraestructura o simplemente porque es preciso atravesar terrenos públicos en los que no es posible tender infraestructura propia. En todos estos casos lo normal es utilizar para la transmisión de los datos los servicios de una empresa portadora. Hasta hace poco este tipo de servicios eran ofrecidos en régimen de monopolio por las compañías telefónicas en la mayoría de los países de Europa.

Las redes WAN se implementan casi siempre haciendo uso de enlaces telefónicos que han sido diseñados principalmente para transmitir la voz humana, ya que este es el principal negocio de las compañías telefónicas. Normalmente la infraestructura está fuera del control del usuario, estando supeditado el servicio disponible a la zona geográfica de que se trate. Conseguir capacidad en redes WAN suele ser caro, por lo que generalmente se solicita el mínimo imprescindible.

Hasta tiempos recientes las conexiones WAN se caracterizaban por su lentitud, costo y tasa de errores relativamente elevada. Con la paulatina introducción de fibras ópticas y líneas digitales en las infraestructuras de las compañías portadoras las líneas WAN han reducido apreciablemente su tasa de errores, también se han mejorado las capacidades y reducido los costos. A pesar del inconveniente que en ocasiones pueda suponer el uso de líneas telefónicas tienen la gran virtud de llegar prácticamente a todas partes, que no es poco.

Con la excepción de los enlaces vía satélite, que utilizan transmisión broadcast, las redes WAN se implementan casi siempre con enlaces punto a punto, por lo que prácticamente todo lo que hemos dicho en el apartado de redes punto a punto es aplicable a las redes WAN.

Redes Inalámbricas y movilidad

En los últimos años ha habido un auge considerable de los sistemas de telefonía inalámbrica.

Algunos usuarios requieren facilidades para conectar por radio enlaces sus computadoras personales desde cualquier lugar o mientras se encuentran viajando en tren, autobús, etc. El sistema de telefonía inalámbrica digital GSM (Global System for Mobile communications), muy extendido en Europa, utiliza un canal digital para transmitir la voz, por lo que es posible conectar una computadora portátil mediante un teléfono GSM, sin necesidad de modem. En algunos países ya se han hecho experimentos de conexiones inalámbricas a 64 Kbps utilizando una versión modificada del GSM

La conexión de computadoras con total movilidad es importante en aplicaciones tales como flotas de taxis, camiones, autobuses, servicios de emergencia, fines militares, etc. En estos casos se emplean, además de las ya familiares computadoras portátiles conocidas como "laptops", otros aún más pequeños que se conocen como "palmtop", asistente digital personal o PDA (Personal Digital Assistant), y que son algo intermedio entre una computadora portátil y una agenda electrónica

Las redes inalámbricas también tienen utilidad en algunos casos donde no se requiere movilidad, como en las LANs inalámbricas. Por ejemplo, una empresa que desea establecer una nueva oficina y por rapidez, provisionalidad de la ubicación o simples razones estéticas no desea cablear el edificio puede utilizar una LAN inalámbrica, consistente en una serie de equipos transmisores-receptores. Las LAN inalámbricas son generalmente más lentas que las normales (1-2 Mbps) y tienen una mayor tasa de errores, pero para muchas aplicaciones pueden ser adecuadas

La movilidad es importante también en casos en que no hay involucradas conexiones inalámbricas.

Por ejemplo un representante que desee conectar con su oficina desde su computadora portátil cuando se encuentra de viaje puede optar por llamar a su oficina directamente, pagando posiblemente una costosa llamada de larga distancia, o bien puede llamar al punto de presencia (POP, Point Of Presence) más próximo de algún proveedor de servicios de comunicación, y a través de este acceder a su oficina por una infraestructura compartida que le resulte más barata (por ejemplo la Internet), en este último caso se dan una serie de problemas de solución no trivial en cuanto a la segundad y el correcto encaminamiento del tráfico.

Internetworking

ejemplo, una LAN (que normalmente será una red de tipo broadcast) casi siempre dispondrá de un router que la interconecte a una WAN (que generalmente consistirá en un conjunto de enlaces punto a punto). Esta interconexión de tecnologías diferentes se conoce como "internetworking" (que podríamos intentar traducir como "interredes"). El router que interconecta redes diferentes está físicamente conectado a todas las redes que se desean interconectar.

Ademas de la combinación de medios físicos diversos es posible encontrarse con necesidades de internetworking en un mismo medio físico; este es el caso cuando coexisten protocolos de comunicación diferentes; por ejemplo, en una misma red Ethernet puede haber unas computadoras utilizando el protocolo TCP/IP y otros utilizando DECNET (protocolo típico de la marca de computadoras Digital). Al ser protocolos diferentes son completamente independientes y no se pueden hablar entre sí, por lo que un usuario de una computadora TCP/IP no podría por ejemplo enviar un mensaje de correo electrónico a uno de una computadora DECNET. Sin embargo, es posible instalar en una computadora ambos protocolos, y un programa de conversión de correo electrónico, de forma que los usuarios de ambas redes puedan intercambiar mensajes. A la máquina que interconecta el correo electrónico de los dos protocolos se le denomina gateway.

Generalmente los gateway han de implementarse a nivel de aplicación; así disponer en nuestro ejemplo de un gateway para el correo electrónico no significa que podamos transferir archivos entre maquinas TCP/IP y DECNET, ya que para esto haría falta un gateway del servicio de transferencia de archivos. Una misma maquina puede actuar como gateway para varios servicios. Haciendo una analogía podemos decir que los protocolos son como idiomas y los gateways equivalen a servicios de traducción que permiten entenderse a personas que hablan diferentes lenguas

Cuando una red esta formada por la interconexión de varias redes se le denomina Internet. A principios de los setenta se creo en los Estados Unidos una Internet mediante la unión de varias redes que utilizando medios de transmisión diversos empleaban un conjunto común de protocolos en el nivel de red y superiores, denominados TCP/IP. Con el tiempo la denominación Internet (con I mayúscula) termino convirtiéndose en el nombre propio de dicha red, muy conocida en nuestros días.

2.4 Cableado Estructurado. Norma ANSI/TIA/EIA-606

Cableado Estructurado

Es la organización de cables dentro de un edificio que recoge las necesidades de comunicación (teléfonos, computadoras, fax, modems, etc.)

Un sistema de cableado esta determinado por el tipo de cable y la topología del sistema. Mientras que el tipo de cable decide la manera de realizar el sistema, la topología decide los costos de instalación, los costos de la futura expansión, así como en algunos casos la complejidad de modificaciones puntuales dentro de la red

A la hora de realizar el cableado de un edificio hay que tener en cuenta que la tecnología varía a tal velocidad que las nuevas tendencias pueden hacer quedar obsoleta cualquier solución adoptada que no prevea una gran capacidad de adaptabilidad.

Por este motivo aparece el concepto de "cableado estructurado". Su intención es:

- Capacidad de crecimiento a bajo costo .
- Base para soportar las tecnologías de niveles superiores sin necesidad de diferentes tipos de cableado.
- Realizar una instalación compatible con las tecnologías actuales y las que estén por llegar.
- Tener la suficiente flexibilidad para realizar los movimientos internos de personas y máquinas dentro de la instalación.
- Estar diseñado e instalado de tal manera que permite una fácil supervisión, mantenimiento y administración.

Topologías en el cableado estructurado

El cableado estructurado reduce todas a las topologías a una sola, la estrella. Todos los puntos se unirán a través de los elementos de interconexión física a un único punto. Esto puede ser así porque cualquier topología se puede convertir en una estrella.

El cableado estructurado consiste por tanto en fijar una disposición física del cable en una instalación, de tal modo que se optimicen al máximo las posibilidades en una red LAN y nos permita una gran facilidad de manejo y migración a nuevas tecnologías y situación física de los usuarios y servidores.

Normatividad para el cableado estructurado

El sistema de cableado constituye el nivel de infraestructura básica de una red de comunicaciones corporativa, su buen diseño y correcta instalación son de suma importancia teniendo en cuenta que es una de las principales causas que pueden afectar al buen funcionamiento de una red.

Un sistema de cableado estructurado tiene (en su parte física) dos partes fundamentales y en este sentido están fijados por las normas

- Por un lado tenemos el cable en si mismo y las normas exigen para cada cable y para cada modo de funcionamiento unas determinadas formas de comportamiento, fundamentalmente relacionadas con la velocidad de trasmisión, la longitud del cable y la atenuación que se produce en la señal

- Por otra parte tenemos el modo de conexión del cable, fijándose una serie de recomendaciones en el sentido de hacer lo más común para todas las instalaciones la manera de conectar los distintos subsistemas que forman parte de la red.

El origen de la norma de cableado estructurado y sobre la cual se hace referencia más a menudo es la ANSI/EIA/TIA 568 (son tres comités de regulación, de electrónica y de telecomunicaciones de EEUU). Esta norma fue establecida en el año 1991 y tiene el título de estandard para el cableado de telecomunicaciones en edificios comerciales.

Existen otra normas del mismo ente que regulan mediciones, fibra óptica, canalizaciones, administración, puesta a tierra entre otros. La norma anterior fue avalada internacionalmente por la ISO/IEC 11801 (ente internacional de estandards y comisión electrotécnica) en el año 1993.

568 Commercial Building Telecommunications Cabling Standard Cableado estructurado para edificios comerciales.

569 Commercial Building Standards for Telecommunications Pathways and Spaces. Especifica los estándares para los conductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones.

570 Residential and Light Commercial Telecommunicationes Wiring Standard. Especifica normas para la instalación de sistemas de telecomunicaciones en residencia y comercios de baja densidad.

607 Commercial Building Grounding and Bonding Requirements for Telecommunications. Regula las especificaciones sobre los sistemas de tierra para equipos de telecomunicaciones.

Norma ANSI/TIA/EIA-606

"Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales". Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Seguir esta norma, permite una mejor administración de una red, creando un método de seguimiento de los traslados, cambios y adiciones.

Objetivo

El estándar 606 reconoce la importancia de una adecuada documentación de la infraestructura de telecomunicaciones para facilitar una correcta administración de la instalación de cable durante su periodo de vida, incluyendo cables, dispositivos de conexión, rutas, espacios y facilidades de telecomunicaciones.

Esquema

El estándar 606 se compone de ocho secciones y cuatro anexos informativos. Al igual que en los estándares 568-A y 569, las tres primeras secciones proporcionan el objetivo, el alcance y disposiciones adoptadas por el documento. El cuerpo principal del estándar lo constituyen las secciones de la cuatro a la ocho. Los anexos proporcionan información útil para la interpretación y aplicación del estándar, además de definir los documentos que han servido para su desarrollo.

Sinopsis

- Sección 1, Introducción - proporciona la idea y objetivo del estándar. Para una eficiente administración y mantenimiento de una compleja (o no tan compleja) infraestructura de telecomunicaciones se realizan tareas de documentación que se actualizarán cada vez que se produzcan movimientos, ampliaciones y cambios una vez instalado el sistema.

- Sección 2, General - discute el alcance del estándar (qué cubre y qué no cubre) y otros estándares normativos que son parte de los requerimientos del 606.

- Sección 3, Definiciones - proporciona una lista de palabras, términos, acrónimos y abreviaciones que se emplean en el documento 606 y sus significados aplicados al documento. Se añade una lista de ejemplos de designaciones que pueden usarse en un sistema de administración.

- Sección 4, Conceptos de Administración - define los tres componentes principales que constituyen el concepto de administracion: identificadores, enlaces y registros.

- Sección 5, Administración de Espacios y Rutas - especifica la forma en que se etiquetan y administran las rutas y espacios. Continua discutiendo sobre informes, dibujos y resúmenes y su aplicación como recursos a la hora de hacer ordenes de trabajo.

- Sección 6, Administración del Sistema de Cableado - discute con mas detalle el uso y ubicación de identificadores, concretamente el de la nomenclatura empleada para identificar cada posicion de terminación de los dispositivos terminales como paneles y bloques de conexión.

- Sección 7, Administracion de Puesta a Tierra/Terminacion - especifica como administrar y etiquetar el sistema de puesta a tierra

- Sección 8, Etiquetado y Codificacion con Colores - discute con mas detalle requerimientos de etiquetado, comenzando por clasificar las etiquetas en adhesivos, módulos y otros.

Anexos

- Anexo 1, Ejemplo de Esquema de Administración en soporte de papel - basándose en una estructura comercial ficticia, consistente en un edificio con seis oficinas, sótano, planta baja y cuatro plantas, ofrece el ejemplo de su administración.

- Anexo 2, Puenteo - se refiere a la administración de circuitos puenteados; cuando un circuito aparece en más de un lugar. El anexo establece claramente que el puenteo no es práctica permitida por el estándar 568, pero que puede ser necesaria su administración en casos especiales.

- Anexo 3, Símbolos de la Infraestructura - proporciona un glosario de símbolos de infraestructura de telecomunicaciones que pueden emplearse en el desarrollo de dibujos previos o posteriores a la construcción.

- Anexo 4, Referencias - proporciona una lista de los estándares referenciados en el cuerpo principal y en los anexos del documento 606.

CAPÍTULO III

ESTÁNDARES Y PROTOCOLOS EN ARQUITECTURAS DE RED

CAPITULO III

ESTANDARES Y PROTOCOLOS EN ARQUITECTURAS DE RED

3.1 Estándares

En nuestra vida diaria estamos rodeados de estándares, incluso para las cosas más triviales como los calibres de cable o el tamaño de las hojas de papel. En algunos casos el estándar hace la vida más cómoda, por ejemplo el formato A4 para la impresión de documentos, permite una manipulación cómoda de estos, en otros es necesario para asegurar la interoperabilidad (la rosca de una tuerca en un tornillo, por ejemplo). Los estándares en materia de telecomunicaciones pertenecen al segundo tipo, es decir, son esenciales para asegurar la interoperabilidad entre diversos fabricantes, cosa esencial si se quieren hacer redes abiertas. Los estándares pueden ser de ámbito regional, nacional o internacional; por ejemplo en Estados Unidos el formato habitual de papel no es el A4 sino tamaño carta (un poco más pequeño) que constituye un estándar nacional.

Las telecomunicaciones son probablemente la primera actividad humana en la que se reconoció la necesidad de definir estándares internacionales.

Conviene destacar que la pertenencia de un país a una determinada organización no asegura su adhesión a los estándares emanados de la misma. Por ejemplo, el tamaño de papel A4 es parte de un estándar de la ISO (International Organization for Standardization) que es seguido por prácticamente todos los países del mundo excepto Estados Unidos que utiliza en su lugar el tamaño carta, a pesar de que también es miembro de la ISO.

Generalmente suele distinguirse dos tipos de estándares: de facto y de jure. Los estándares de facto (del latín "del hecho") ocurren cuando un determinado producto o modo de comportamiento se extiende en una comunidad determinada sin una planificación previa, hasta el punto de que ese producto o modo de comportamiento se considera "normal" dentro de esa comunidad. Los estándares de facto ocurren de forma natural y progresiva, sin una planificación previa ni un proceso formal que los sustente. Por ejemplo en aplicaciones de oficinas informáticas es un estándar de facto la computadora compatible IBM con software de Microsoft; en entornos universitarios de docencia e investigación en informática es un estándar de facto el uso de sistemas operativo UNIX. Los estándares de facto también se llaman a veces "estándares de la industria".

Los estándares de jure (del latín "por ley") son fruto de un acuerdo formal entre las partes implicadas, después de un proceso de discusión, consenso y generalmente votación. Se adoptan en el seno de una organización que normalmente está dedicada a la definición de estándares; si dicha organización tiene ámbito internacional el estándar definido es internacional. Existen dos clases de organizaciones internacionales: las "oficiales" que son fruto de tratados internacionales y que se crean por acuerdo entre los gobiernos de las naciones participantes, y las "extraoficiales", que existen gracias al esfuerzo voluntario de sus miembros, sin participación directa de los gobiernos de sus países.

En el mundo de las redes de computadoras existen hoy en dia como hemos visto dos conjuntos de protocolos estándar, el OSI y el TCP/IP, pero ambos son relativamente recientes. En los años setenta y ochenta en que no habia protocolos estándar disponibles la forma más sencilla de constituir una red multifabricante era utilizando los protocolos de IBM: SNA (Sistem Network Architecture) o su predecesor el NJE (Network Job Entry), como los equipos IBM eran los más extendidos casi todos los fabricantes disponian de productos que implementaban estos protocolos en sus equipos, con lo que jugaban el papel de protocolos "estándar"; además, en muchos casos una buena parte de las computadoras a conectar era IBM por lo que el software necesario estaba alli de todos modos. Podemos decir que en aquellos años los protocolos SNA y NJE era hasta cierto punto un estándar de facto

Muchos paises tienen organizaciones nacionales de estándares donde expertos de la industria y las universidades desarrollan estándares de todo tipo. Entre ellas se encuentran por ejemplo:

- ANSI American National Standards Institute (Estados Unidos)
- DIN Deutsches Institut fuer Normung (Alemania)
- BSI British Standards Institution (Reino Unido)
- AFNOR Association Francaise de Normalisation (Francia)
- UNI Ente Nazionale Italiano de Unificatione (Italia)
- NNI Nederlands Normalisatie-Instituut (Paises Bajos)
- SAA Standards Australia (Australia)
- SANZ Standards Association of New Zealand (Nueva Zelanda)
- DS Dansk Standard (Dinamarca)
- AENOR Asociación Española de Normalización (España)

La ISO es una organización voluntaria, es decir, no es fruto de tratados internacionales, creada en 1946 con sede en Ginebra, Suiza. Sus miembros son las organizaciones nacionales de estándares de los 89 paises miembros. A menudo un estándar de uno de sus miembros es adoptado por ISO como estándar internacional; esto ocurre especialmente con las más importantes, ANSI, DIN, BSI y AFNOR.

ISO emite estándares sobre todo tipo de asuntos, como por ejemplo: el sistema métrico de unidades de medida, tamaños de papel, sobres de oficina, tornillos y tuercas, reglas para dibujo técnico, conectores eléctricos, regulaciones de seguridad, componentes de bicicleta, números ISBN (International Standard Book Number), lenguajes de programación, protocolos de comunicación, etc. Hasta la fecha se han publicado unos 10 000 estándares ISO que afectan a prácticamente cualquier actividad de la vida moderna.

Para realizar esta inmensa labor ISO se organiza en cerca de 200 comités técnicos (TC, Technical Committee) numerados según su creación. El TC97 trata de computadoras y proceso de la información. Cada comité tiene subcomités (SCs) que a su vez se dividen en grupos de trabajo (WG, Working Groups)

ISO ha generado multitud de estándares en Telemática, y en tecnologías de la información en general, siendo OSI[1] su ejemplo más significativo. Además, ha adoptado estándares producidos por sus organizaciones miembros y por otras organizaciones relacionadas.

La ITU (International Telecommunication Union) fue creada en 1934, y con la creación de la ONU se vinculó a ésta en 1947. La ITU tiene tres sectores de los cuales sólo nos interesa el que se dedica a la estandarización de las telecomunicaciones, que se conoce como ITU-T. Desde 1956 a 1993 la ITU-T se conoció con el nombre CCITT, acrónimo del nombre francés (Comité Consultatif International Télégraphique et Téléphonique). En 1993 la CCITT fue reorganizada y se le cambió el nombre a ITU-T; estrictamente hablando el cambio de nombre tiene efectos retroactivos, es decir, los documentos vigentes, aun cuando fueran producidos antes de 1993, son hoy documentos de la ITU-T y no de la CCITT.

Los miembros de la ITU-T son de cinco clases:

- Administraciones (PTTs nacionales).
- Operadores privados reconocidos (por ejemplo British Telecom, Global One, AT&T).
- Organizaciones regionales de telecomunicaciones (por ejemplo el ETSI).
- Empresas que comercializan productos relativos a telecomunicaciones y organizaciones científicas.
- Otras organizaciones interesadas (bancos, líneas aéreas, etc.).

Entre los miembros hay unas 200 administraciones, unos cien operadores privados y varios cientos de miembros de las otras clases. Sólo las administraciones tienen derecho a voto, pero todos los miembros pueden participar en el trabajo. Cuando un país no tiene un monopolio de comunicaciones, como Estados Unidos, no existe PTT y la representación recae en algún organismo del gobierno relacionado (esto será posiblemente lo que ocurra ahora en la mayoría de los países de Europa).

Las tareas de la ITU-T comprenden la realización de recomendaciones sobre interfaces de teléfono, telégrafo y comunicaciones de datos. A menudo estas recomendaciones se convierten en estándares reconocidos internacionalmente, por ejemplo la norma V.24 (también conocida como EIA RS-232) que especifica la posición y el significado de las señales en el conector utilizado en muchos terminales asíncronos.

La ITU-T denomina a sus estandares "recomendaciones"; con esto se quiere indicar que los países tienen libertad de seguirlas o ignorarlas; aunque ignorarlas puede suponer quedar aislado del resto del mundo, por lo que en la práctica a menudo las recomendaciones se traducen en obligaciones.

[1] Vease capitulo 3.4 "Modelo OSI"

Entre las recomendaciones más relevantes de la ITU-T en el campo de la Telemática podemos destacar la serie V sobre modems (por ejemplo V.32, V.42), la serie X sobre redes de datos y OSI (X.25, X.400,...), las series I y Q que definen la RDSI, la serie H sobre codificación digital de sonido y vídeo, etc.

Internet Society

Cuando se puso en marcha la ARPANET[2] el DoD creó un comité que supervisaba su evolución. En 1983 dicho comité recibió el nombre de IAB (Internet Activities Board), nombre que luego se cambió a Internet Architecture Board. Este comité estaba constituido por diez miembros. Dada la naturaleza de las organizaciones que constituían la ARPANET (y después la NSFNET) los miembros del IAB representaban básicamente a universidades y centros de investigación.

El IAB informaba de la evolución de la red y las posibles mejoras a realizar. El IAB también se ocupaba de detectar después de intensas discusiones- donde era necesario o conveniente especificar un nuevo protocolo; entonces se anunciaba dicha necesidad en la red y normalmente siempre surgían voluntarios que lo implementaban. La información circulaba en forma de documentos técnicos denominados RFCs (Request For Comments). El nombre da una idea del talante abierto y democrático que tienen todas las actividades de la Internet. Los RFCs se mantienen en la red y cualquiera que lo desee puede consultarlos, redistribuirlos, etc. (como comparación diremos que los documentos de la ITU y la ISO solo pueden obtenerse comprandolos a la oficina correspondiente); actualmente hay mas de 2000 RFCs y su número crece continuamente.

En 1989 el IAB fue reorganizado de nuevo para acomodarse a la evolución sufrida por la red. Su composición fue modificada para que representara a un rango más amplio de intereses ya que la anterior resultaba muy académica, y tenía un procedimiento de nombramiento no democrático (los miembros salientes nombraban a sus sucesores). Además se crearon dos subcomités dependientes del IAB, el IRTF (Internet Research Task Force) y el IETF (Internet Engineering Task Force); el IRTF se concentraría en los problemas a largo plazo, mientras que el IETF debía resolver las cuestiones de ingeniería más inmediatas.

En 1991 se creo la Internet Society (ISOC), una asociación internacional para la promoción de la tecnología Internet y sus servicios. Cualquier persona física u organización que lo desee puede ser miembro de la ISOC sin más que pagar su cuota anual. La ISOC está gobernada por un consejo de administración (Board of Trustees) cuyos miembros son elegidos por votación de los miembros de la ISOC entre una serie de candidatos propuestos. La ISOC absorbió en su seno el IAB con sus dos subcomités, pero cambió radicalmente el mecanismo de elección; estos son ahora nombrados por el consejo de administración de la ISOC

Dentro de la compleja estructura que es la ISOC el grupo más importante en lo que a elaboración de estándares se refiere es sin lugar a dudas el IETF. Inicialmente éste se dividió en grupos de trabajo, cada uno con un problema concreto a resolver. Los presidentes de dichos grupos de trabajo se reunían regularmente constituyendo lo que se llamaba el Comité Director.

[2] Véase capítulo 1 "Antecedentes Históricos"

A medida que fueron apareciendo problemas nuevos se fueron creando grupos de trabajo, llegando a existir más de 70 con lo que se tuvieron que agrupar en ocho áreas; el Comité Director está formado ahora por los ocho presidentes de área.

Paralelamente a la modificación de las estructuras organizativas se modificaron también los procedimientos de estandarización, que antes eran muy informales. Una propuesta de nuevo estándar debe explicarse con todo detalle en un RFC y tener el interés suficiente en la comunidad Internet para que sea tomada en cuenta; en ese momento se convierte en un Estándar Propuesto (Proposed Standard). Para avanzar a la etapa de Borrador de Estándar (Draft Standard) debe haber una implementación operativa que haya sido probada de forma exhaustiva por dos instalaciones independientes al menos durante cuatro meses. Si el IAB se convence de que la idea es buena y el software funciona declarará el RFC como un *Estándar Internet (Internet Standard)*. El hecho de exigir implementaciones operativas probadas antes de declarar un estándar oficial pone de manifiesto la filosofía pragmática que siempre ha caracterizado a Internet, radicalmente opuesta a ISO e ITU-T.

Foros industriales

El proceso de definicion de estándares de los organismos internacionales "tradicionales" (ITU-T e ISO) siempre se ha caracterizado por una gran lentitud, debida quizá a la necesidad de llegar a un consenso entre muchos participantes y a procedimientos excesivamente complejos y burocratizados. La lentitud en crear los estándares OSI fue uno de los factores que influyó en su rechazo. El caso de RDSI es extremo: la ITU-T empezó a elaborar el estándar en 1972, y lo finalizó en 1984; los servicios comerciales aparecieron hacia 1994, 22 años después de iniciado el proceso; este retraso provocó que lo que se diseño como un servicio avanzado para su tiempo (accesos digitales a 64 Kbps) resultara cuando se puso en marcha aprovechable sólo en entornos domesticos y de pequeñas oficinas.

Estos retrasos producian grandes pérdidas a los fabricantes de equipos, que no estaban dispuestos a repetir el error. Por ello a principios de los noventa empezó a surgir un nuevo mecanismo para acelerar la creación de estandares, consistente en la creación de grupos independientes formados por fabricantes, usuarios y expertos de la industria con un interés común en desarrollar una tecnologia concreta de forma que se garantice la interoperabilidad de los productos de diversos fabricantes. Esto es lo que se conoce como foros industriales.

Los foros no pretenden competir con las organizaciones internacionales de estándares, sino cooperar con ellas y ayudarlas a acelerar su proceso, especialmente en la parte más difícil, la que corresponde a la traduccion de los documentos en implementaciones que funcionen en la práctica.

Generalmente los foros trabajan en los mismos estandares intentando aclarar ambiguedades y definir subconjuntos de funciones que permitan hacer una implementación sencilla en un plazo de tiempo mas corto y comprobar la viabilidad y la interoperabilidad entre diversos fabricantes; así los organismos de estandarizacion pueden disponer de prototipos reales del estándar que se esta definiendo. En cierto modo es como traer a la ISO e ITU-T el estilo de funcionamiento de la IETF.

Otra característica de los foros es que se establecen fechas límite para la producción de estándares, cosa que no hacen los organismos oficiales; de esta manera los fabricantes pueden planificar la comercialización de sus productos de antemano, ya que saben para qué fecha estarán fijados los estándares necesarios.

Entre las tecnologías que se han estandarizado o se están estandarizando por este procedimiento están Frame Relay, ATM, ADSL (Asymmetric Digital Subscriber Loop) y algunas variantes de Ethernet de alta velocidad, como el gigabit Ethernet forum que está especificando las características de una versión de Ethernet a 1 Gbps. El ATM forum, creado en 1991 por Northern Telecom, Sprint, Sun Microsystems, y Digital Equipment Corporation (DEC), cuenta en la actualidad con mas de 500 miembros.

Otras organizaciones

El IEEE (Institute of Electrical and Electronics Engineers) es una asociación profesional de ámbito internacional. Aparte de otras muchas tareas el IEEE (también llamado IE cubo) tiene un grupo sobre estandarización que desarrolla estándares en el área de ingeniería eléctrica e informática. Entre estos se encuentran los estándares 802 que cubren prácticamente todos los aspectos relacionados con la mayoría de los sistemas habituales de red local. Los estándares 802 han sido adoptados por ISO con el número 8802.

El NIST (National Institute of Standards and Technology) es una agencia del Departamento de Comercio de los Estados Unidos, antes conocido como el NBS (National Bureau of Standards). Define estándares para la administración de los Estados Unidos.

El ANSI es la organización de estándares de los Estados Unidos. La única razón de mencionarlo es porque a menudo sus estándares son adoptados por ISO como estándares internacionales.

El ETSI (European Telecommunications Standards Institute) es una organización internacional dedicada principalmente a la estandarización de las telecomunicaciones europeas. Es miembro de la ITU-T. Entre sus misiones está elaborar especificaciones detalladas de los estándares internacionales adaptadas a la situación de Europa en los aspectos históricos, técnicos y regulatorios.

La EIA (Electrical Industries Association) es una organización internacional que agrupa a la industria informática y que también participa en aspectos de la elaboración de estándares.

La ECMA (European Computer Manufacturers Association), creada en 1961, es un foro de ámbito europeo donde expertos en proceso de datos se ponen de acuerdo y elevan propuestas para estandarización a ISO, ITU-T y otras organizaciones.

La CEPT (Conference European of Post and Telecommunications) es una organización de las PTTs europeas que participa en la implantación de estándares de telecomunicaciones en Europa. Sus documentos se denominan Norme Europeene de Telecommunication (NET). La CEPT está avalada por la Comunidad Europea.

Estandarización en México

Un estándar no sólo es importante para los aspectos operativos de una red o un sistema de telecomunicaciones, sino también para cumplir con la regulación y normatividad vigente en el país. Un estándar tal como lo define la ISO (International Organization for Standardization) "son acuerdos (normas) documentados que contienen especificaciones técnicas y otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". Por lo tanto un estándar de telecomunicaciones "es un conjunto de normas y recomendaciones técnicas que regulan la transmisión en los sistemas de comunicaciones".

La homologación es el acto por el cual la entidad encargada de regular las comunicaciones de un país (en el caso de México es la Comisión Federal de Telecomunicaciones, COFETEL) reconocen oficialmente que las especificaciones de un producto destinado a telecomunicaciones satisfagan las normas y requisitos establecidos, por lo que puede ser conectado a una red pública de telecomunicaciones o hacer uso del espectro radioeléctrico.

Tipos de Homologación

- Homologación Provisional: Vigencia de un año y podrá ser renovado hasta en dos ocasiones.
- Homologación Definitiva : Vigencia indefinida
- Registro de uso exclusivo de Homologación: Vigencia indefinida.

Norma

Norma. Fijación por medio de un acuerdo de los criterios que debe cumplir un equipo de comunicaciones en cuanto a calidad, tipo de material, valores de ciertas características asociadas o del tipo de interfaz de modo que pueda interconectarse a las redes públicas sin problema alguno.

Existen básicamente dos tipos de Normas Oficiales en México:

- NOM (Norma Oficial Mexicana)
- NMX (Normas Mexicanas, acordadas por consenso de la propia industria)

En el caso de las telecomunicaciones, las normas NOM son de dos tipos:

- La primera será competencia de Secretaría de Economía y de sus laboratorios asociados, y se refiere a los aspectos de seguridad alrededor del producto.
- La segunda norma trata el aspecto de la operación del aparato, para evitar, por ejemplo: interferencias entre concesionarios en el caso de que se use el espectro radioeléctrico.

En México se homologan todos aquellos equipos que se interconectan a la red pública de telecomunicaciones, tales como aparatos telefónicos, modems, conmutadores, multicanalizadores, radios VHF, UHF, radios de microondas, amplificadores de potencia, antenas de satélite y microondas, etc. El equipo de cómputo no requiere homologación, sólo de NOM.

Los vendedores de equipos y las empresas. Los primeros deben de estar obligados a vender equipos con homologación en México, en caso de que no se tenga el certificado de homologación, deben tramitar un certificado provisional. En el caso de las empresas para cumplir con la normatividad deberan homologar sus equipos bajo un registro exclusivo de homologación. Existen bases de datos donde se puede verificar que equipos están actualmente homologados.

Para obtener una homologación de un equipo de comunicaciones en México, deberá presentarse documentación técnica (avalada por un perito en comunicaciones) a la COFETEL con los siguientes requisitos: descripción general del equipo, descripción de los parámetros técnicos, interfaces con las vías de comunicación y dictamen técnico.

El proceso de homologacion pretende mas que nada reglamentar y registrar todos aquellos equipos que estarán conectados con las redes públicas, así como administrar y regular los equipos que hagan uso del espectro electromagnético. Los administradores de redes de las empresas, antes de comprar cualquier equipo de comunicaciones, deben solicitarle al vendedor el certificado de homologación y evitarse así los trámites, pérdidas de tiempo y dinero del trámite de la homologacion

3.2 Protocolos

Los protocolos es el conjunto de reglas que gobiernan el intercambio de datos entre dos entidades. Se utilizan para la comunicación entre entidades de diferentes sistemas.

Los términos Entidad y Sistema se utilizan en un sentido muy general. Ejemplos de entidades son programas de aplicacion de usuario, paquetes de transferencia de archivos, sistemas de manejo de bases de datos y terminales. Ejemplos de sistemas son computadoras, terminales y sensores remotos. En general, una entidad es *algo* capaz de enviar o de recibir información, y un sistema es un objeto que contiene una o más entidades. Para que dos entidades puedan comunicarse deben hablar el mismo idioma. ¿Qué se comunica?, ¿cómo se comunica? y ¿cuando se comunica? deben cumplir ciertas convenciones entre las entidades involucradas; este conjunto de convenciones constituye un protocolo

La tarea de la comunicación entre dos entidades de diferentes sistemas es demasiado complicada para ser manejada por un simple proceso o módulo En lugar de manejar un único protocolo, implementaremos las funciones de comunicacion mediante un conjunto de protocolos estructurados. La organización de estos protocolos se realiza mediante una serie de capas o niveles, con objeto de reducir la complejidad de su diseño. Cada una de ellas se construye

sobre su predecesora. El número de capas, el nombre, contenido y función de cada una varían de una red a otra. Sin embargo, en cualquier red, el propósito de capa es ofrecer ciertos servicios a las capas superiores, liberándolas del conocimiento detallado sobre cómo se realizan dichos servicios.

La capa n en una máquina conversa con la capa *n* de otra maquina. Las reglas y convenciones utilizadas en esta conversación se conocen conjuntamente como protocolo de la capa n. A las entidades que forman las capas correspondientes en máquinas diferentes se les denomina procesos pares (igual a igual). En otras palabras, son los procesos pares los que se comunican mediante el uso del protocolo.

En realidad no existe una transferencia directa de datos desde una capa *n* de una máquina a la capa *n* de otra; si no, más bien, cada capa pasa la información de datos y control a la capa inmediatamente inferior, y así sucesivamente hasta que se alcanza la capa localizada en la parte más baja de la estructura. Debajo de la capa 1 está el medio físico, a través del cual se realiza la comunicación real.

Entre cada par de capas adyacentes hay una interfaz, la cual define los servicios y operaciones primitivas que la capa inferior ofrece a la superior. El diseño claro y limpio de una interfaz, además de minimizar la cantidad de información que debe pasarse entre capas, hace más simple la sustitución de la realización de una capa por otra completamente diferente (por ejemplo, todas las líneas telefónicas se reemplazan por canales satelitales).

Las primeras redes de computadoras tuvieron unos inicios muy similares a las primeras computadoras. Las redes y los protocolos se diseñaban pensando en el hardware a utilizar en cada momento, sin tener en cuenta la evolución previsible, ni por supuesto la interconexión y compatibilidad con equipos de otros fabricantes. A medida que la tecnología avanzaba y se mejoraba la red se vivieron experiencias parecidas a las de las primeras computadoras, por ejemplo los programas de comunicaciones, que habían costado enormes esfuerzos de desarrollo, tenían que ser re-escritos para utilizarlos con el nuevo hardware y debido a la poca modularidad prácticamente nada del código era aprovechable

El problema se resolvió de forma análoga a lo que se había hecho con las computadoras. Cada fabricante elaboró su propia arquitectura de red, que permitía independizar las funciones y el software del hardware concreto utilizado. De esta forma cuando se quería cambiar algún componente sólo la función o el módulo afectado tenía que ser sustituido. La primera arquitectura de redes fue anunciada por IBM en 1974, justo diez años despues de anunciar la arquitectura S/360, y se denominó SNA. La arquitectura SNA se basa en la definición de siete niveles o capas, cada una de las cuales ofrece una serie de servicios a la siguiente, la cual se apoya en esta para implementar los suyos, y así sucesivamente. Cada capa puede implementarse en hardware, software o una combinación de ambos. El módulo (hardware y/o software) que implementa una capa en un determinado elemento de la red debe poder sustituirse sin afectar al resto de la misma, siempre y cuando el protocolo utilizado se mantenga inalterado. Dicho en otras palabras, SNA es una arquitectura altamente modular y estructurada. El modelo de capas que utiliza ha sido la base de todas las arquitecturas de redes actualmente

en uso, incluidas las basadas en el modelo OSI y el TCP/IP (Transmission Control Protocol/Internet Protocol).

Las ideas básicas del modelo de capas son las siguientes:

La capa n ofrece una serie de servicios a la capa n+1.

La capa n solo "ve" los servicios que le ofrece la capa n-1.

La capa *n* en un determinado sistema sólo se comunica con su homóloga en el sistema remoto (comunicación de igual a igual o "peer-to-peer"). Esa "conversación" se efectúa de acuerdo con una serie de reglas conocidas como protocolo de la capa n.

La comunicación entre dos capas adyacentes en un mismo sistema se realiza de acuerdo con una interfaz. La interfaz es una forma concreta de implementar un servicio y no forma parte de la arquitectura de la red

La arquitectura de una red queda perfectamente especificada cuando se describen las capas que la componen, su funcionalidad, los servicios que implementan y los protocolos que utilizan para hablar con sus "iguales". El conjunto de protocolos que utiliza una determinada arquitectura en todas sus capas se denomina pila *de* protocolos (Protocol stack), así es frecuente oír hablar por ejemplo de la pila de protocolos OSI, SNA, TCP/IP, etc.

Cuando un sistema desea enviar un mensaje a un sistema remoto normalmente la información se genera en el nivel más alto; conforme va descendiendo se producen diversas transformaciones, por ejemplo adición de cabeceras, de colas, de información de control, la fragmentación en paquetes más pequeños, si es muy grande (o más raramente la fusión con otros si es demasiado pequeño), etc. Todas estas operaciones se invierten en el sistema remoto en las capas correspondientes, llegando en cada caso a la capa correspondiente en el destino un mensaje igual al original.

Decisiones en el diseño de arquitecturas de redes.

Cuando se diseña una arquitectura de red hay una serie de aspectos y decisiones fundamentales que condicionan todo el proceso. Entre estos cabe mencionar los siguientes:

- Direccionamiento: cada capa debe poder identificar los mensajes que envía y recibe. En ocasiones una misma computadora puede tener varias instancias de una misma capa, por lo que la sola identificación de la computadora puede no ser suficiente.

- Normalmente cualquier protocolo admite comunicación en ambos sentidos (dúplex); pero no siempre se permite que esta ocurra de forma simultánea (full-dúplex), también se debe determinar si se definirán prioridades, y cuáles serán éstas.

- En cualquier comunicación es preciso establecer un control de errores, ya que los canales de comunicación no son totalmente fiables. Es preciso decidir que código de

detección y/o corrección de errores se va a utilizar, y en que capa o capas se va a llevar a cabo. Generalmente a medida que los medios de transmisión mejoran y las tasas de errores disminuyen la detección/corrección se va suprimiendo de las capas inferiores y dejando al cuidado de las más altas, ya que es un proceso costoso que puede llegar a distorsionar apreciablemente la transmisión.

- En algunos casos se debe tener en cuenta la posibilidad de que los paquetes lleguen a su destino en orden diferente al de envío.

- Debe contemplarse la posibilidad de que el receptor no sea capaz de "digerir" la información enviada por el transmisor. Para esto es conveniente disponer de algún mecanismo de control de flujo y notificación para indicar la congestión.

- Normalmente los equipos funcionan de forma óptima cuando el tamaño de los mensajes que se envían esta dentro de un cierto rango. Para evitar los problemas que puede producir el envío de mensajes muy grandes o muy pequeños se suelen contemplar mecanismos de fragmentación y reagrupamiento. Es importante que estos mecanismos estén claramente especificados para evitar la destrucción del mensaje en tránsito.

Modelos de Referencia

Las dos arquitecturas más importantes en la actualidad, corresponden a los protocolos OSI y TCP/IP. Conviene destacar que la arquitectura es una entidad abstracta, más general que los protocolos o las implementaciones concretas en que luego se materializan éstos.

Típicamente para cada capa de una arquitectura existirán uno o varios protocolos, y para cada protocolo habrá múltiples implementaciones. Las implementaciones cambian continuamente; los protocolos ocasionalmente se modifican o aparecen otros nuevos que coexisten con los anteriores o los dejan anticuados; sin embargo una vez definida una arquitectura ésta permanece esencialmente intacta y muy raramente se modifica.

Protocolo X.25

X.25 fue el primer protocolo estándar de red de datos pública. Se definió por primera vez en 1976 por la CCITT. Aunque el protocolo ha sido revisado múltiples veces (la última en 1993) ya se ha quedado algo anticuado y no es en la actualidad un servicio interesante, salvo en algunos casos, debido a su baja eficiencia y velocidad; normalmente no supera los 64 Kbps, aunque se pueden contratar conexiones de hasta 2 048 Kbps. A pesar de estas desventajas conviene conocer los aspectos básicos de X 25 pues aún existe una gran cantidad de usuarios de este tipo de redes.

Además, en el protocolo X 25 se definieron por primera vez muchos de los conceptos en que se basa Fame Relay y ATM, que podemos considerar en cierto sentido como sus descendientes. El conjunto de estándares que definen X.25 ha sido adoptado como parte del modelo OSI para los tres primeros niveles.

A nivel físico se definen en X.25 dos interfaces, la X.21 cuando se usa señalización digital (cosa poco habitual) y la X.21bis (un subconjunto de la EIA-232D/V.24) cuando es analógica.

A nivel de enlace se utiliza un protocolo llamado LAP-B (Link Access Procedure-Balanced) que es una versión modificada del estándar ISO HDLC (High-level Data Link Control).

El protocolo utilizado a nivel de red se conoce como X.25 PLP (Packet Layer Protocol). En este nivel se realizan todas las funciones de control de flujo, confirmación y direccionamiento. Cada NSAP (Network Services Access Point) en una red X.25 viene representado por una interfaz de un conmutador X.25, y tiene una dirección única. Las direcciones son numéricas y típicamente pueden tener entre nueve y quince dígitos.

Las redes X.25 públicas de muchos países están interconectadas, como ocurre con las redes telefónicas. Para facilitar su direccionamiento la CCITT ha establecido un sistema jerárquico análogo al sistema telefónico en la recomendación X.121.

X.25 es un servicio fiable orientado a conexión; los paquetes llegan en el mismo orden con que han salido. Una vez establecido un circuito entre dos NSAPs la información se transfiere en paquetes que pueden ser de hasta 128 bytes (aunque en muchas redes se permiten tamaños de hasta 4 KB). En la red los paquetes son transferidos de cada conmutador al siguiente (almacenamiento y reenvío), y sólo borrados cuando se recibe la notificación de recepción.

Las computadoras que se conectan a un conmutador X.25 necesitan tener la capacidad suficiente para procesar los complejos protocolos X.25. Cuando se definió el estándar X.25 las computadoras personales eran caras y poco potentes; muchos usuarios que tenían necesidad de conectarse a redes X.25 no disponían de una computadora adecuada. Para estos casos se diseñó un equipo capaz de conectar una terminal asíncrona, que trabaja en modo carácter (es decir, un paquete por carácter) a una red X.25, a dicho equipo se le denominó PAD (Packet Assembler Disassembler) ya que se ocupaba de ensamblar y desensamblar los paquetes X.25 que recibía. A través de un PAD un usuario de una PC, o incluso de un terminal "tonta", podía conectarse a un host en una red X.25 y trabajar como una terminal remota de aquel. La CCITT publicó tres documentos para especificar todo lo relacionado con el funcionamiento de un PAD: el X.3 describe las funciones propias del PAD, el X.28 define el protocolo de comunicación entre el PAD y la terminal asíncrona, y el X.29 define el protocolo entre el PAD y la red X.25. El uso conjunto de estos tres protocolos permite iniciar una sesión interactiva desde un terminal conectada a un PAD con una computadora remota, por lo que se le conoce como el logon remoto XXX. Cuando un usuario en una computadora conectada a X.25 desea establecer una conexión como terminal remota de otra computadora a través de una red X.25 lo hace mediante un programa en su computadora que emula el comportamiento de un PAD (PAD Emulation). El logon remoto XXX ofrece en redes X.25 un servicio equivalente al de Telnet en TCP/IP. Para el caso de usuarios que no dispongan de un PAD propio muchas compañías telefónicas ponen a su disposición un servicio de acceso a PADs por RTC (normalmente RTB). Este servicio se denomina normalmente X.28, por ser este estándar el que define el protocolo de comunicaciones entre la terminal de usuario y el PAD.

El rendimiento que se obtiene de un VC (Virtual Circuit) X.25 depende de muchos factores: velocidad de los accesos físicos implicados, número de VC simultáneos, tráfico en cada uno de ellos, carga de la red, infraestructura, etc.

Los protocolos X.25 se diseñaron pensando en los medios de transmisión de los años setenta, líneas de baja velocidad con tasa de errores elevada. El objetivo era aprovechar lo mejor posible las lentas líneas de transmisión existentes, aún a costa de hacer un protocolo de proceso pesado.

Por si esto fuera poco, las redes X.25 casi siempre se utilizan para encapsular tráfico correspondiente a otros protocolos, por ejemplo TCP/IP, SNA o DECNET (podríamos decir que los paquetes de estos protocolos viajan "disfrazados" en paquetes X.25); cuando se encapsula un protocolo como TCP/IP en X.25 se realizan de forma redundante las tareas de la capa de red, con lo que el resultado es aún más ineficiente.

Para resolver este tipo de problemas a partir de 1990 se empezaron a crear redes basadas en Frame Relay.

Frame Relay

Frame Relay (que significa retransmisión de tramas) nació a partir de los trabajos de estandarización del servicio RDSI, como un intento de crear una versión "light" de X.25, que permitiera aprovechar las ventajas de poder definir circuitos virtuales pero sin la baja eficiencia que tenían los protocolos excesivamente "desconfiados" de X.25.

Mientras que en X.25 la capa de enlace y la capa de red eran sumamente complejas en Frame Relay ambas se intentaron reducir a su mínima expresión, dejando en manos de los equipos finales toda la labor de acuse de recibo, retransmisión de tramas erróneas y control de flujo; de esta forma Frame Relay se convertía en el complemento perfecto a otros protocolos, tales como TCP/IP. En muchos casos se considera que Frame Relay no es un protocolo a nivel de red sino a nivel de enlace (de ahí su nombre), y aun visto como nivel de enlace resulta bastante ligero.

El servicio que suministra Frame Relay consiste básicamente en identificar el principio y final de cada trama y detectar errores de transmisión. Si se recibe una trama errónea simplemente se descarta, confiando en que el protocolo de nivel superior de los equipos finales averigüe por sí mismo que se ha perdido una trama y decida si quiere recuperarla, a diferencia de X.25, Frame Relay no tiene control de flujo ni genera acuse de recibo de los paquetes (estas tareas también se dejan a los niveles superiores en los equipos finales), el tamaño máximo de los paquetes varía según las implementaciones entre 1 KB y 8 KB. La velocidad de acceso a la red típicamente está entre 64 y 2.048 Kbps, aunque ya se trabaja la estandarización de velocidades del orden de 34 Mbps.

Una novedad importante de Frame Relay estriba en que se define un ancho de banda "asegurado" para cada circuito virtual mediante un parámetro conocido como CIR (Committed Information Rate). Un segundo parámetro, conocido como EIR (Excess Information Rate) define

el margen de tolerancia que se dará al usuario, es decir, cuanto se le va a dejar "pasarse" del CIR contratado.

Por ejemplo, si una computadora se conecta a una red Frame Relay mediante una línea de acceso al conmutador de 1.984 Kbps, y tiene dos circuitos establecidos con otras dos computadoras, cada uno de ellos con un CIR de 256 Kbps y un EIR de 256 Kbps; en este caso cada circuito tendrá asegurado un ancho de banda de 256 Kbps como mínimo, y si la red no está saturada podrá llegar a 512 Kbps; si un circuito intenta utilizar más de 512 Kbps el conmutador Frame Relay empezará a descartar tramas. En este caso la línea de acceso nunca llegaría a saturarse, ya que máximo podrían enviarse 512 Kbps por cada circuito. La especificación del CIR para un circuito virtual se hace de forma independiente para cada sentido de la transmisión, y puede hacerse asimétrica, es decir dar un valor distinto del CIR para cada sentido.

Cuando un usuario hace uso del EIR (es decir, genera un tráfico superior al CIR contratado en un circuito virtual) el conmutador Frame Relay pone a 1 en las tramas excedentes, un bit especial denominado DE (Discard Elegibility). Si se produce congestión en algún punto de la red el conmutador en apuros descartará en primera instancia las tramas con el bit DE marcado, intentando resolver así el problema. Este mecanismo permite a un usuario aprovechar la capacidad sobrante en la red en horas valle sin perjudicar la calidad de servicio a otros usuarios en horas pico, ya que entonces se verá limitado a su CIR. En realidad el CIR tampoco está garantizado, ya que si la congestion no se resuelve descartando las tramas DE el conmutador empezará a descartar tramas normales (no marcadas como DE) que pertenecen a usuarios que no han superado su CIR. Afortunadamente las redes Frame Relay se suelen dimensionar de forma que el CIR de cada usuario esté prácticamente garantizado en cada momento. En cierto modo podemos imaginar el bit DE como un sistema de "reserva de asiento" en un billete de tren (el bit a 0 significaría en este caso tener hecha la reservación).

Una red Frame Relay podría utilizarse en vez de líneas dedicadas para interconectar conmutadores X.25; a la inversa sería mucho más difícil ya que al ser X.25 una red más lenta los retardos introducidos serían apreciados por los usuanos de Frame Relay.

En ocasiones se utilizan redes Frame Relay para transmitir voz digitalizada; esto no es posible con X.25 debido a la lentitud del protocolo, que introduciría unos retardos excesivos; el envío de voz por una red tiene unos requerimientos especialmente severos en cuanto a retardos para que la transmisión se efectúe correctamente.

ATM y B-ISDN

Casi todos los servicios de comunicación que hemos visto hasta ahora fueron diseñados para la transmisión de voz o datos, pero no ambos. La RTB y la red GSM, pensadas para la voz, pueden transmitir datos, pero sólo a muy bajas velocidades. Las líneas dedicadas y redes Frame Relay, pensadas para datos, pueden transmitir voz si se utilizan los equipos apropiados y se respetan ciertas restricciones

El único servicio de los que se ha visto hasta ahora que se diseñó pensando en voz y datos es la RDSI (de ahí el nombre de Servicios Integrados). Pero la RDSI tiene dos inconvenientes importantes:

1. Al ser una red de conmutación de circuitos *reales* la reserva del ancho de banda se realiza durante todo el tiempo que esta establecida la comunicación, independientemente de que se estén transfiriendo datos o no (o en el caso de transmitir voz independientemente de que se este hablando o se este callado).

2. El estándar RDSI se empezo a definir en 1984. En aquel entonces las lineas dedicadas eran de 9.6 Kbps en el mejor de los casos y hablar de enlaces a 64 Kbps parecía algo realmente avanzado; sin embargo el proceso de estandarización tardó más de lo previsto (cosa que ocurre a menudo) y cuando aparecieron los primeros servicios RDSI diez años más tarde la red "avanzada" resultaba interesante sólo en entornos domésticos y de pequeñas oficinas; se había quedado corta para nuevas aplicaciones.

Las redes de comunicaciones permiten transmitir también otros tipos de información como imágenes en movimiento (videoconferencia o vídeo), que tienen unos requerimientos distintos. De una forma muy concisa se resume en la siguiente tabla las caracteristicas esenciales de cada tipo de tráfico:

Tipo de información	Capacidad	Pérdida tolerable	Retardo	Jittter
Datos	Variable	Muy baja	Alto	Alto
Audio en tiempo real, monólogo	Baja (64 Kbps)	Baja	Bajo	Muy bajo
Audio en tiempo real, diálogo	Baja (64 Kbps)	Baja	Muy bajo	Muy bajo
Video en tiempo real	Alta (2 Mbps)	Media	Bajo	Bajo

En 1986 la CCITT definio el concepto de RDSI-BA y eligió ATM como la tecnología sobre la que se basarían los futuros estándares. En aquel entonces ATM era una tecnología que interesaba exclusivamente a las compañías telefónicas. Gradualmente los fabricantes de computadoras se fueron percatando de las posibilidades y futuro de dicha tecnología; para acelerar el proceso de estandarización se creó en 1991 el ATM forum, en el que participaban compañías telefónicas y fabricantes de computadoras. A partir de ese momento se ha producido un avance impresionante en las normas y equipos ATM, especialmente en lo que se refiere a redes de datos. El primer conmutador ATM comercial apareció en 1991

Las compañías telefonicas vienen trabajando desde hace bastante tiempo en el diseño de una red adecuada al trafico multimedia que permita aprovechar las ventajas de la conmutacion de

paquetes, para así utilizar de forma más eficiente las infraestructuras y ofrecer servicios nuevos, tales como la videoconferencia o el video bajo demanda. La tecnología que permite todo esto se denomina ATM (Asynchronous Transfer Mode) y sus orígenes se remontan nada menos que a 1968, cuando se concibió en los laboratorios Bell el primer sistema de transmisión de celdas. En esencia lo que se intenta con esta nueva tecnología es integrar todos los servicios en una única red digital, lo mismo que pretendía la RDSI (aunque como hemos visto llegó demasiado tarde). Por este motivo ATM también se denomina a veces RDSI de banda ancha o RDSI-BA (B-ISDN, Broadband-ISDN); por contraste a la "antigua" RDSI se la denomina en ocasiones RDSI de banda estrecha o RDSI-BE (N-ISDN, Narrowband-ISDN). La RDSI de banda ancha es lo más parecido a las "autopistas de la información".

En cierto sentido ATM puede verse como una evolución de Frame Relay. La principal diferencia es que los paquetes ATM tienen una longitud fija de 53 bytes (5 de cabecera y 48 de datos) frente al tamaño variable y mucho mayor de las tramas Frame Relay.

Debido a su tamaño pequeño y constante los paquetes ATM se denominan celdas, y por esto en ocasiones a ATM se le denomina cell relay (retransmisión de celdas).

Manejar celdas de un tamaño tan reducido tiene la ventaja de que permite responder con mucha rapidez a tráfico de alta prioridad que pueda llegar inesperadamente mientras se están transmitiendo otros menos urgentes, algo muy importante en tráfico multimedia. El hecho de que todas las celdas sean del mismo tamaño simplifica el proceso en los nodos intermedios, cuestión esencial cuando se quiere que dicho proceso sea lo más rápido posible. En el lado negativo está el hecho de que la eficiencia de una conexión ATM nunca puede superar el 90% (48/53) debido a la información de cabecera que viaja en cada celda.

Al igual que en X.25 o Frame Relay, una red ATM se constituye mediante conmutadores ATM normalmente interconectados por líneas dedicadas, y equipos de usuario conectados a los conmutadores. Mientras que en X.25 o Frame Relay se utilizan velocidades de 64 Kbps a 2 Mbps, en ATM las velocidades pueden llegar a 155,52, 622,08 o incluso superiores. La elección de precisamente estos valores se debe a que son los que se utilizan en el nuevo sistema de transmisión sobre fibra óptica en redes WAN denominado SONET/SDH (Synchronous Optical NETwork/Synchronous Digital Hierarchy), que es el que están utilizando las compañías telefónicas actualmente en las infraestructuras. ATM también puede utilizarse a velocidades inferiores, 34 Mbps e incluso 2 Mbps.

Dos equipos conectados a una red ATM pueden establecer entre sí un circuito virtual, permanente o conmutado, y transmitir por él información digital de cualquier tipo. ATM da al usuario muchas mas facilidades que X.25 o Frame Relay para controlar las características de su circuito virtual; se puede fijar un ancho de banda máximo permitido, un margen de tolerancia sobre dicho máximo, un ancho de banda mínimo garantizado, un ancho de banda asimétrico, un perfil horario de forma que el ancho de banda fluctúe con la hora del día de una forma preestablecida, etc. Además es posible definir prioridades y distintos tipos de tráfico, de forma que se prefiera fiabilidad o rapidez, tráfico constante o a ráfagas, etc.

El modelo de referencia ATM

ATM tiene su propio modelo de referencia, constituido por tres capas denominadas capa física, capa ATM y capa de adaptación ATM, o capa AAL (ATM Adaptation Layer).

La capa física está formada por dos subcapas: la PMD (Physical Media Dependent) y la TC (Transmission Convergence). La subcapa PMD describe la interfaz física con el medio de transmisión, y equivale a la capa física del modelo OSI. La subcapa TC se ocupa de "deshacer" las celdas en bits para pasarlos a la subcapa PMD en el envío, y de recibir los bits de la subcapa PMD para reconstruir las celdas en la recepción. Si consideramos la celda como equivalente a la trama en el modelo OSI ésta subcapa haría la función de la capa de enlace.

La capa ATM trata de la estructura de las celdas y su transporte. También realiza las tareas de señalización, es decir establece y termina los circuitos virtuales, y realiza el control de congestión. Sus funciones son una mezcla de la capa de enlace y la capa de red en el modelo OSI.

La capa de adaptación ATM (capa AAL) se divide también en dos subcapas; la inferior se denomina subcapa SAR (Segmentation And Reassembly) se ocupa de fragmentar el paquete que recibe desde arriba (normalmente mayor de 48 bytes) en celdas para su envío, y de reensamblarlo en la recepción cuando se lo pasa la capa ATM. La subcapa CS (Convergence Sublayer) se ocupa de suministrar distintos tipos de servicio adecuados al tipo de tráfico (video, audio, datos etc.). La capa AAL corresponde en sus funciones a la capa de transporte del modelo OSI.

En el modelo de referencia ATM no se habla de aplicaciones. En realidad el modelo contempla la existencia de capas por encima de la capa AAL, pero no se especifican sus funciones ni características. El modelo deja total libertad a los implementadores sobre como diseñar las aplicaciones que funcionen sobre ATM. Actualmente el principal uso de ATM es como medio de transporte para otros protocolos; hay muy pocas aplicaciones que hayan sido diseñadas para funcionar de manera nativa.

HDLC - High-level Data Link Control

En 1972 IBM desarrolló un protocolo de enlace denominado SDLC (Synchronous Data Link Protocol) para utilizarlo en las redes SNA. A pesar de su antiguedad SDLC es la base de la mayoría de los protocolos de enlace que se utilizan en la actualidad.

Posteriormente IBM propuso la estandarización de SDLC a ANSI e ISO; cada uno de estos organismos introdujo sus propias variantes sobre la propuesta inicial, dando así un conjunto de protocolos similares pero no idénticos. El creado por ANSI se denomina ADCCP (Advanced Data Communication Control Procedure), el de ISO se llama HDLC (High level Data Link Control); CCITT creo LAP (Link Access Procedure) y más tarde LAPB (Link Access Procedure Balanced, también llamado Link Access Procedure versión B) que es un subconjunto de HDLC que se utiliza por ejemplo en X.25. Para la señalización (es decir, el establecimiento de la

llamada) en RDSI la CCITT creó otro subconjunto de HDLC denominado LAPD (Link Access Procedure D-channel). Frame Relay a su vez utiliza una variante de LAPD. Podemos considerar a todos estos protocolos como una familia cuyo miembro más representativo es el HDLC.

La estructura de la trama HDLC es como sigue:

Campo	Tamaño (bits)	Valor
Delimitador	8	01111110
Dirección	8	Variable
Control	8	Variable
Datos	>=0	Variable
Checksum	16	Variable
Delimitador	8	01111110

La trama se delimita mediante la secuencia 01111110, y para asegurar la transparencia de datos se utiliza relleno de bits (bit stuffing), es decir, se intercala un bit a 0 cuando en la parte de datos aparece una secuencia de cinco bits a 1, procediendo de modo inverso en el lado receptor; esto asegura la no-ambigüedad en la identificación del principio y final de la trama. Cuando la línea no está transmitiendo tramas útiles los equipos envían continuamente la secuencia (01111110111111101111110....). Cada trama puede tener cualquier longitud a partir de 32 bits (sin contar los delimitadores), pudiendo no ser múltiplo de 8, ya que no se presupone una estructura de bytes. Por esto se suele decir que HDLC es un protocolo orientado al bit (en contraste con los requieren que la trama sea múltiplo de 8, que se denominan orientados al byte).

El campo datos, también llamado en ocasiones carga útil (payload) puede o no estar presente; puede contener cualquier información y tener cualquier longitud, si bien la eficiencia del checksum disminuye cuando la longitud aumenta.

El campo dirección sólo se utiliza en líneas multipunto. Las líneas multipunto son conexiones en las que varias computadoras comparten una misma línea física, lo cual es poco frecuente y requiere líneas especiales; en las líneas multipunto hay una computadora que actúa de "moderador" dando el turno de palabra a los demás (en cierto modo podemos considerarlas como precursoras de las redes broadcast). El campo dirección permite identificar a cual de todas las computadoras accesibles en la línea va dirigida la trama.

El campo control es realmente el corazón del protocolo. Su primer bit especifica el tipo de trama que lo contiene, que puede ser de información o de supervisión. Las tramas de información son las únicas que contienen datos. En el campo control envía un número de secuencia de tres bits que se utiliza para un protocolo de ventana deslizante de tamaño máximo 7; el mecanismo utilizado puede ser de retroceso n o de retransmisión selectiva. En cada trama de información se incluye un acuse de recibo (ACK) piggybacked que ocupa tres bits en el campo control (recordemos que el ACK tiene que ser del mismo tamaño que el número de secuencia).

Las tramas de supervisión pueden ser de varios tipos:

Tipo 0: RECEIVE READY. Es el nombre que recibe en el estándar el acuse de recibo (ACK). Se utiliza cuando no hay tráfico de retorno suficiente para utilizar piggybacking.

Tipo 1: REJECT. Corresponde al acuse de recibo negativo (NAK). Solicita retransmisión de una trama, y no acepta ninguna otra entre tanto. Se utiliza cuando se emplea el mecanismo de retroceso n.

Tipo 2: RECEIVE NOT READY. Indica un acuse de recibo pero solicita suspensión del envío para evitar saturar al receptor (control de flujo), cosa que puede ser necesaria si el receptor tiene poco espacio para buffers. Para que la retransmisión se reanude debe enviar un RECEIVE READY, REJECT o ciertas tramas de control.

Tipo 3: SELECTIVE REJECT. Se utiliza para solicitar retransmisión de una trama determinada cuando se emplea retransmisión selectiva. En este caso por tanto la ventana del emisor con un número de secuencia de tres bits no puede ser mayor de 4. Este mecanismo solo está previsto en HDLC y ADCCP, no en SDLC ni LAPB.

En HDLC y LAPB existe un tipo de trama extendida en la que los números de secuencia son de 7 bits; en este caso es posible utilizar un tamaño de ventana de hasta 127 usando la técnica de retroceso n o de 64 usando la de repetición selectiva.

3.3 Protocolos para acceso a Internet

El nivel de enlace en la Internet

El modelo TCP/IP dice muy poco acerca del nivel de enlace; desde hace bastante tiempo está especificado como transportar paquetes IP sobre redes locales, redes X.25, etc., pero sorprendentemente el transporte de paquetes IP sobre líneas serie (dedicadas o RTC) se ha efectuado durante mucho tiempo con protocolos particulares, y no ha sido estandarizado hasta epoca reciente.

SLIP - Serial Line IP

Este es el más antiguo de los dos protocolos y data de 1984. Se trata de un protocolo muy sencillo que utiliza un caracter como indicador, y caracteres de relleno en caso de que dicho carácter aparezca en la trama. Debido a su sencillez solo se utiliza en conexiones conmutadas.

Algunas versiones recientes de SLIP llevan a cabo la compresión de la información de cabecera TCP e IP; esto se hace porque a menudo paquetes consecutivos tienen muchos campos de cabecera comunes.

SLIP no genera un CRC, y por tanto no es posible detectar tramas erróneas; cualquier error ha de ser corregido por los niveles superiores. Evidentemente esto simplifica enormemente las implementaciones pero reduce de forma apreciable el rendimiento.

Además del problema de la detección de errores SLIP tiene una serie de inconvenientes importantes que lo hacen inapropiado para cualquier utilización mínimamente seria; su uso está decayendo rápidamente en favor del PPP, mucho más avanzado.

A pesar de haberse publicado como un RFC (1055), SLIP no es un Internet Standard.

PPP

Para mejorar la situación el IETF puso en marcha un grupo de trabajo que elaborara un protocolo de enlace que pudiera llegar a ser un estándar Internet. El resultado fue un protocolo elaborado en 1990 denominado PPP (Point-to-Point Protocol) definido en los RFC 1661, 1662 y 1663.

PPP ha sido diseñado para ser muy flexible; para ello incluye un protocolo especial, denominado LCP (Link Control Protocol), que se ocupa de negociar una serie de parámetros en el momento de establecer la conexión con el sistema remoto.

La estructura de trama de PPP se basa en la de HDLC, salvo por el hecho de que se trata de un protocolo orientado a carácter, por lo que la longitud de la trama ha de ser un número entero de bytes

Campo	Tamaño (bytes)	Valor
Delimitador	1	01111110
Dirección	1	11111111
Control	1	00000011
Protocolo	1 ó 2	Protocolo
Datos	>=0	Variable
Checksum	2 ó 4	Variable
Delimitador	1	01111110

Dado que el protocolo es orientado a carácter, la ocurrencia del delimitador 01111110 dentro de la trama se resuelve con relleno de caracter, duplicando el carácter correspondiente.

El campo dirección no se utiliza. Siempre vale 11111111.

El campo control tiene por defecto el valor 00000011, que indica una trama no numerada. Esto significa que por defecto PPP no suministra transmisión fiable (con números de secuencia y

acuse de recibo, como hemos visto para HDLC). Aunque no es lo normal, en el momento de establecer la conexión LCP puede negociar una transmisión fiable.

Salvo que se negocie una transmisión fiable los campos dirección y control contienen siempre la secuencia 11111111100000011. Dado que es inútil transferir esta información de control que siempre contiene la misma información, generalmente LCP negocia la supresión de estos dos bytes de la trama al inicio de la sesión cuando no se pide transmisión fiable.

El campo *protocolo* establece a que tipo de protocolo pertenece el paquete recibido de la capa de red. De esta forma PPP permite establecer una comunicación multiprotocolo, es decir puede utilizarse para transmitir paquetes pertenecientes a diferentes protocolos del nivel de red entre dos computadoras simultaneamente. Entre las posibilidades se encuentra IP, IPX (Novell), Appletalk, DECNET, OSI y otros.

El campo *datos* es de una longitud variable hasta un máximo que negocia LCP al establecer la conexión; por defecto el tamaño máximo de trama es de 1500 bytes.

El campo checksum es normalmente de 2 bytes, pero puede ser de 4 si se negocia.

Igual que ocurre en la vida real, la negociación entre dos LCPs puede dar lugar a que todos los valores propuestos sean aceptados por la otra parte, o solo algunos de ellos. El protocolo establece mecanismos que permiten a los LCPs dialogar para llegar a un consenso en caso de discrepancia.

LCP suministra mecanismos que permiten validar a la computadora que llama (mediante el uso de claves tipo usuario/password). Esto resulta especialmente útil en el caso de conexiones por RTC, por ejemplo para proveedores de servicios Internet que han de facturar a sus usuarios en función del tiempo de conexión.

Existe otro componente de PPP que es el NCP (Network Control Protocol). Este se encarga de negociar los parametros especificos para cada protocolo utilizado. Por ejemplo, en el caso de una conexion IP desde un usuario conectado via modem le asigna dinámicamente una dirección IP, lo cual es especialmente util en casos en que el número de direcciones IP disponibles sea menor que el numero de usuarios del servicio (aunque por supuesto el número de direcciones IP disponibles debe ser suficiente para poder asignar una diferente a cada usuario simultáneo).

PPP es un mecanismo de transporte de tramas multiprotocolo que puede utilizarse sobre medios físicos muy diversos, por ejemplo conexiones mediante modem y RTC, RDSI, lineas dedicadas, o incluso por conexiones SONET/SDH de alta velocidad (aunque esto último no es normal).

El nivel de enlace en ATM lo que para nuestro modelo hibrido OSI-TCP/IP es el nivel de enlace corresponde en el modelo ATM a lo que se denomina la subcapa TC (Transmission Convergence, convergencia de la transmision) y que allí se incluye como parte de la capa física. La tarea fundamental de dicha subcapa TC es, la obtencion de las celdas provenientes de la

capa ATM (capa de red) y su transformación en una secuencia de bits a transmitir que pasa a la subcapa PMD (Physical Media Dependent) la cual hace la función del nivel físico en nuestro modelo.

En el comité de la CCITT que elaboraba los estándares ATM existían dos grupos claramente diferenciados. Por un lado estaban los fabricantes de computadoras, así como empresas y organismos interesados en usar ATM para crear redes de datos; estos eran reacios a utilizar un tamaño de celda pequeño, ya que esto introduce un elevado costo de proceso y una pérdida considerable de capacidad debido a las cabeceras que necesariamente ha de llevar cada celda. Este grupo proponía un tamaño de celda de 128 bytes.

En la postura contraria se encontraban las PTTs europeas, cuyo objetivo era utilizar ATM para transmitir conversaciones telefónicas. Además de utilizar la técnica habitual PCM para digitalizar una conversación telefónica en un canal de 64 Kbps, en ATM es bastante frecuente utilizar técnicas de compresión (por ejemplo la denominada ADPCM) que permiten meter el canal habitual en tan solo 32, o incluso 24 Kbps. De esta forma es posible aprovechar aun más la capacidad disponible.

Las PTTs proponían utilizar celdas de 16 bytes, ya que así una conversación podría generar una celda cada 2 ms si se usaba PCM, o cada 4 o 6 ms si se empleaba ADPCM. Con celdas de 128 bytes como proponían los fabricantes de computadoras costaría 16 ms llenar una celda con una conversación PCM, y 32 o 48 ms con ADPCM; ahora bien, si la celda tarda mas de 20 ms en llenarse se produciría un efecto de eco similar al de una conexión telefónica de muy larga distancia (mas de 2.000 Km), ya que el llenado de la celda esta produciendo en este caso un retardo equivalente al del cable en la conexion a larga distancia; por tanto es preciso instalar costosos equipos de cancelacion de eco.

Las compañías telefónicas estadounidenses no tenían ningun problema con la utilización de celdas de 128 bytes, ya que con retardos de mas de 30 ms en las comunicaciones costa a costa estaban ya desde hacia tiempo instalando canceladores de eco en sus líneas. Pero las PTTs europeas, al trabajar con distancias menores de 2.000 Km, no han instalado canceladores de eco y en caso de haber optado por celdas de 128 bytes se habrían visto obligadas a hacer costosas inversiones, o a renunciar a la posibilidad de utilizar sistemas de compresión para transmitir la voz, como ADPCM

Después de muchas negociaciones cada bando cedio un poco en sus pretensiones.

Las PTT accedieron a subir a 32 bytes el tamaño de celda, mientras que los fabricantes de computadoras bajaron a 64 bytes. En ese momento la CCITT decidio terminar la discusión partiendo la diferencia y fijando la celda en 48 bytes (más cabecera). Así utilizando ADPCM a 24 Kbps el retardo puede llegar a ser de 18ms, que esta muy cerca del límite de 20 ms para que se produzca el eco (hay que tomar en cuenta que además habra alguna longitud de cable cuyo retardo también influye).

Transmisión de celdas

Cada celda ATM tiene 5 bytes de cabecera, el último de los cuales es un checksum de los otros cuatro. La subcapa TC se ocupa de calcular el valor de dicho byte utilizando el polinomio generador $x^8 + x^2 + x + 1$. Este campo checksum se denomina HEC (Header Error Control).

La razón de hacer checksum de la cabecera únicamente es acelerar el proceso de cálculo; se supone que los niveles superiores harán corrección de errores si lo consideran apropiado (algunas aplicaciones, como el video o audio, pueden soportar sin problemas una pequeña tasa de errores).

También debemos tomar en cuenta el hecho de que ATM se diseñó pensando en las fibras ópticas, que son un medio de transmisión altamente fiable. Hay estudios que demuestran que la gran mayoría de los (ya pocos) errores que se producen en fibras ópticas son errores simples. El HEC detecta todos los errores simples y el 90% de los errores múltiples.

Una vez está en su sitio el HEC la celda está lista para transmisión. Existen dos tipos de medios de transmisión, los asíncronos y los síncronos. Los asíncronos simplemente transmiten cada celda cuando esta preparada. Los síncronos por el contrario tienen que transmitir celdas con una periodicidad fija, y en caso de no haber celdas útiles preparadas envían celdas de relleno o inútiles (también llamadas "idle" cells).

Otro tipo de celdas "anormales" (es decir, sin datos) son las denominadas celdas OAM (Operation And Maintenance). Estas son utilizadas por los conmutadores ATM para intercambiar información de control sobre la red, con la que es posible hacer labores de mantenimiento, tales como gestión de averías y de rendimiento. Sirven también para transmitir información del estado de la red, por ejemplo del grado de congestion. También se utilizan celdas OAM para "saltar" el espacio ocupado por la información de control de una trama SONET/SDH.

Recepción de celdas

En el lado receptor la subcapa TC ha de tomar el flujo de bits entrante, localizar el principio y final de cada celda, verificar el HEC (y descartar las celdas inválidas), procesar las celdas OAM y las celdas inútiles, y pasar a la capa ATM las celdas de datos.

La detección del principio y final de cada celda se hace por mecanismos completamente distintos a los utilizados en HDLC. No existe ninguna secuencia de bits característica del principio y final de cada celda, pero si se sabe que cada celda ocupa exactamente 53 x 8 = 424 bits, por lo que una vez localizada una será facil encontrar las siguientes. La clave para encontrar la primera celda está en el HEC: en recepción la subcapa TC captura 40 bits de la secuencia de entrada y parte de la hipótesis de que sea un principio de celda válido; si lo es el cálculo del HEC será correcto, si no desplaza la secuencia un bit y repite el cálculo; repitiendo este proceso como máximo 424 veces el TC localiza finalmente el principio de una celda, y a partir de ella todas las que le siguen.

Con un HEC de 8 bits la probabilidad de que un conjunto de bits elegido al azar resulte ser un HEC válido es de 1/256, lo cual no es despreciable. Por tanto la TC, para asegurar que su hipótesis no ha sido fruto de la casualidad, repite el cálculo con el HEC siguiente; haciendo esta comprobación con varias celdas sucesivas se puede reducir a un nivel despreciable la probabilidad de que el acierto haya sido pura casualidad. Por ejemplo si el resultado es correcto en cinco celdas consecutivas la probabilidad de que esto sea fruto de la casualidad es de $1/256^5$, o sea 10^{-12} aproximadamente.

Una vez localizado el principio de una celda la TC ya puede sin problemas localizar todas las demás por su posición relativa, siempre que se mantenga el sincronismo.

Podría ocurrir que como consecuencia de un error se introdujera o eliminara un bit en la secuencia, con lo que la TC perdería el sincronismo. En tal caso el primer síntoma sería un HEC erróneo, pero un HEC erróneo puede significar un bit erróneo, cosa más normal que un bit de más o de menos. Por esto cuando la TC detecta un HEC erróneo no supone inmediatamente que ha perdido el sincronismo; en principio considera que ha sido un bit erróneo, y se pone alerta ante la posibilidad de que la siguiente celda dé también un HEC erróneo, en cuyo caso la sospecha de pérdida de sincronismo crece.

Si varias celdas consecutivas tienen un HEC erróneo la TC supone que ha perdido el sincronismo por algún motivo y empieza de nuevo el proceso de detección de principio de celda.

Cabe pensar en la posibilidad de que un usuario genere, con o sin intención, flujos de datos con secuencias de 5 bytes que al incluirlos en celdas ATM contuvieran sistemáticamente HECs válidos; entonces la TC podría interpretar erróneamente la cabecera de celdas, y por tanto los datos. Para evitar esta posibilidad los bits de datos son reorganizados o revueltos (scrambled) antes de efectuar transmisión y reordenados en la recepción, para regenerar la información original. Esta reorganización se hace de forma que los datos del usuario no puedan interferir el proceso normal de detección del principio y final de las celdas

Debido a la preocupación reciente por el agotamiento inminente del conjunto actual de direcciones de Internet y el deseo de proporcionar funcionalidad adicional para dispositivos modernos, se encuentra en proceso de normalización una actualización de la versión actual del Protocolo Internet (IP, Internet Protocol) denominada Ipv4 La nueva versión, denominada IP versión 6 (IPv6), resuelve problemas de diseño no previstos en Ipv4. Aquí se describen los problemas de Internet Ipv4 y cómo los resuelve Ipv6 . Aquí se presenta los fundamentos de los conceptos de Ipv6 basados en estándares de Internet

La versión actual de IP (conocida como versión 4 o IPv4) no ha cambiado sustancialmente desde la publicación de RFC 791 en 1981. IPv4 ha demostrado su robustez, facilidad de implementación e interoperabilidad, y ha superado la prueba que representa ampliar una red interna para convertirla en un servicio global de las dimensiones actuales de Internet. Esto es un tributo a su diseño inicial.

Sin embargo, en el diseño inicial no se previó lo siguiente:

El reciente crecimiento exponencial de Internet y el inminente agotamiento del espacio de direcciones IPv4.

Las direcciones IPv4 son relativamente escasas, lo que ha obligado a algunas organizaciones a utilizar el Traductor de direcciones de red (NAT, Network Ardes Translator) para asignar múltiples direcciones privadas a una sola dirección IP pública.

Aunque NAT permite reutilizar el espacio de direcciones privadas, no admite la seguridad basada en estándares en la capa de red o la asignación correcta de todos los protocolos de nivel superior y puede crear problemas cuando se conectan dos organizaciones que utilizan el espacio de direcciones privadas.

Además, la creciente proliferación de dispositivos y aparatos conectados a Internet apunta a que el espacio de direcciones públicas de IPv4 se agotará dentro de un tiempo.

El crecimiento de Internet y la capacidad de los enrutadores troncales de Internet para mantener grandes tablas de enrutamiento.

Debido a la forma en la que se asignan los Id de red IPv4, existen normalmente más de 70.000 rutas en la tabla de enrutamiento de los enrutadores troncales de Internet. La infraestructura actual del enrutamiento de IPv4 en Internet es una combinación de enrutamiento plano y jerárquico.

La mayor parte de las implementaciones actuales de IPv4 deben configurarse manualmente o mediante un protocolo de configuración de direcciones con estado, como el Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). Ante un número mayor de equipos y dispositivos que utilizan IP, existe la necesidad de emplear una configuración de direcciones más sencilla y automática, así como otros parámetros de configuración no basados en la administración de una infraestructura DHCP.

El requisito de seguridad en el nivel de IP

La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que protejan los datos que se envían ante posibles observaciones o modificaciones durante el tránsito. Aunque ahora existe un estándar para ofrecer seguridad a los paquetes de IPv4 (conocida como seguridad de Protocolo Internet o IPSec), es opcional y prevalecen las soluciones propietarias.

La necesidad de facilitar la entrega de datos en tiempo real, también denominada calidad de servicio (QoS, Quality of Service).

Aunque existen estándares de QoS para IPv4, el tráfico en tiempo real se basa en el campo Type of Service (TOS o Tipo de servicio) de IPv4 y en la identificación de la carga, normalmente mediante un puerto UDP o TCP. Por desgracia, el campo Type of Service de IPv4 presenta una

funcionalidad limitada y con el tiempo han surgido distintas interpretaciones locales. Además, la identificación de la carga mediante un puerto TCP y UDP no es posible cuando la carga de paquetes IPv4 está cifrada.

Dada esta problemática, el IETF (Internet Engineering Task Force) desarrolló un conjunto de protocolos y estándares a los que llamó IPv6. El nuevo diseño del IP ha sido pensado para que afecte lo menos posible a los protocolos de nivel superior e inferior al evitar que se agreguen aleatoriamente nuevas características.

3.4 Modelo OSI

Introducción

El modelo de referencia para la Interconexión de Sistemas Abiertos (OSI, Open System Interconnection), también conocido con la denominación ISA (Interconexión de Sistemas Abiertos), fue aprobado por ISO, Organización internacional de normalización y estandarización, en el año 1984 bajo la norma ISO 7498, después de 5 años de duro trabajo. Con posterioridad el CCITT lo incorporó a las recomendaciones de la serie X, bajo la denominación X.200.

El modelo OSI surge de la necesidad imperante de interconectar sistemas de procedencia diversa, distintos fabricantes, cada uno de los cuales empleaba sus propios protocolos para el intercambio de señales. El término abierto se seleccionó con la idea de realzar la facilidad básica del modelo que dio origen al mismo, frente a otros modelos "propietarios" y, por tanto, cerrados.

El concepto OSI o ISA está descrito en las normas ISO 7498-1 e ITU-T X.200. Los estandares OSI describen las reglas que deben seguir los equipos de comunicaciones para que el intercambio de datos sea posible dentro de una infraestructura que esté compuesta de una gran variedad de productos de diferentes suministradores. A partir de ese modelo se han desarrollado una gran familia de protocolos para que diferentes tipos de computadoras puedan trabajar y comunicarse conjuntamente sobre diversos tipos de redes.

Conceptos básicos de OSI

Para reducir la complejidad de su diseño, muchas redes están organizadas como una serie de capas o niveles, cada una construida sobre la anterior. El numero de capas y el nombre, el contenido y la función de cada una difieren de red a red. Sin embargo, en todas las redes el propósito de cada capa es ofrecer ciertos servicios a las capas superiores de modo que no tengan que ocuparse del detalle de la implementacion real de los servicios. Es decir, las entidades del nivel n suministran un servicio a las entidades del nivel n+1. Los servicios se encuentran disponibles en las SAP (Service Access Point). Cada SAP tiene una dirección que lo identifica y que permiten a la capa n+1 acceder a los servicios que se ofrecen. A un mismo SAP pueden estar conectados varios procesos, cada una de ellos a un punto final de conexión.

La capa n de una máquina lleva a cabo una conversación con la capa n de otra. Las reglas y convenciones que se siguen en esta conversación se conocen colectivamente como protocolo de capa n. Básicamente, un protocolo es un acuerdo entre las partes que se comunican sobre cómo va a proceder la comunicación. En caso de que se viole el protocolo, la comunicación puede llegar a ser muy difícil, sino imposible.

Las entidades que comprenden las capas correspondientes en las diferentes máquinas se denominan entidades pares. Es decir, son los pares los que se comunican usando el protocolo.

Pero en realidad, los datos no se transfieren directamente de la capa n de una máquina a la capa n de otra. Más bien, cada capa pasa datos e información de control a la capa que está inmediatamente debajo de ella, hasta llegar a la capa más baja. Bajo la capa 1 está el medio físico a través del que ocurre la comunicación real. En otras palabras, la comunicación lógica es horizontal, pero la comunicación física es vertical.

Entre cada par de capas adyacentes hay una interfaz. La interfaz define qué operaciones y servicios primitivos ofrece la capa inferior a la superior. Una de las consideraciones importantes de diseño es definir interfaces claras entre capas. Esto requiere que cada capa ejecute una colección específica de funciones bien conocidas.

Además de minimizar la cantidad de información que se debe pasar entre capas, las interfaces bien definidas también simplifican el reemplazo de la implementación de una capa con una implementación completamente diferente, pues todo lo que se requiere de la nueva implementación es que ofrezca a su vecino de arriba exactamente el mismo conjunto de servicios que ofrecía la implementación vieja.

Las capas pueden ofrecer dos tipos diferentes de servicio a las capas que se encuentran sobre ellas:

- Servicio orientado a la conexión: encuentra su modelo en el sistema telefónico. Para conversar con alguien, descolgamos el teléfono, marcamos el número, hablamos y después colgamos. De manera similar, para usar un servicio de red orientado a la conexión, el usuario del servicio establece primero una conexión, la usa y después la libera. El aspecto esencial de una conexión es que actúa como un tubo: el emisor empuja objetos (bits) por un extremo y el receptor los saca en el mismo orden por el otro extremo.

- Servicio sin conexión: encuentra su modelo en el sistema de correo postal. Cada mensaje (carta) lleva la dirección completa del destino, y cada uno se encamina a través del sistema de forma independiente de todos los demás. Normalmente, cuando se envían dos mensajes al mismo destino, el primero que se envió será el primero en llegar. Sin embargo, es posible que el primero que se envió se retrase tanto que el segundo llegue primero. Con un servicio orientado a la conexión esto es imposible.

Cada servicio se puede caracterizar por una calidad de servicio. Algunos servicios son confiables en el sentido de que nunca pierden datos. Usualmente, un servicio confiable se implementa haciendo que el receptor haga acuse de recibo de cada mensaje, de modo que el emisor esté seguro de que llegó. El proceso de acuse de recibo introduce una sobrecarga y retardos que con frecuencia valen la pena pero que algunas veces son intolerables.

Una situación típica en la que un servicio confiable orientado a la conexión es apropiado es la transferencia de archivos. El propietario del archivo quiere asegurarse de que todos y cada uno de los bits lleguen correctamente y en el mismo orden en que se enviaron. Muy pocos clientes de transferencia de archivos preferirían un servicio que perdiera algunos bits ocasionalmente aun si fuera mucho más rápido.

Los servicios y protocolos son conceptos distintos, aunque con frecuencia se les confunde. Un servicio es un conjunto de operaciones primitivas que ofrece una capa a la que está por encima de ella. El servicio define cuáles son las operaciones que la capa está preparada para ejecutar en beneficio de sus usuarios, pero nada dice respecto de cómo se van a instrumentar estas operaciones. El servicio se refiere a la interfaz entre dos capas, siendo la capa inferior la que provee el servicio y la capa superior la que hace uso de él.

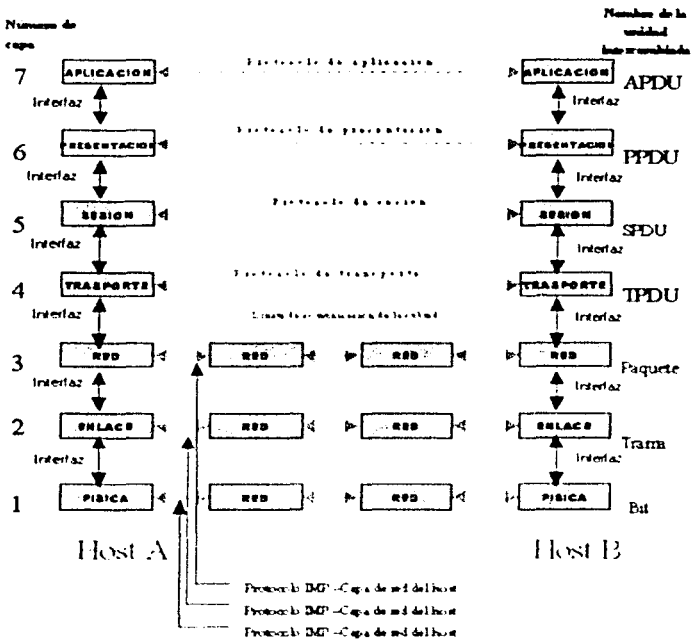
Estructura en niveles

Concepto de nivel.

Con el objetivo de definir un estándar flexible y con posibilidades de ampliarse, los organismos de normalización pensaron que era una buena idea para conseguirlo, el separarlo en varios módulos.

Cada módulo se encarga de unas tareas específicas por lo que resulta mucho más fácil realizar cambios en una parte sin que se tenga alterar el resto de las especificaciones. Así el modelo OSI consta de 7 capas o niveles como se muestra en la siguiente figura:

MODELO OSI



Los principios que se aplicaron para llegar a las siete capas son los siguientes:

- Cada capa debe tener un nivel de abstracción diferente.
- Cada capa debe realizar un conjunto de labores perfectamente determinadas.
- La función de cada capa se debe elegir pensando en la definición de protocolos internacionalmente estandarizados.
- La frontera entre capas tiene que estar definida para conseguir que el flujo de información entre niveles sea el mínimo.

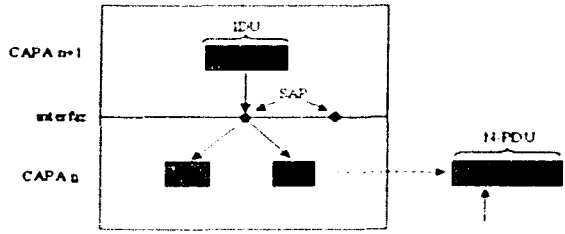
- Compromiso en el número de niveles.
- Concepto de proveedor y de usuario de servicio.
- La función de cada capa es proporcionar servicios a la capa que está encima de ella. Los elementos activos de cada capa generalmente se llaman entidades.
- Los servicios están disponibles en los SAP (Service Access Points, puntos de acceso al servicio).

Los SAP de la capa n son los lugares en los que la capa n+1 puede tener acceso a los servicios ofrecidos. Casa SAP tiene una dirección que lo identifica de manera única. Para aclarar este punto, los SAP del sistema telefónico son los enchufes en los que se pueden conectar los teléfonos modulares, y las direcciones de los SAP son los números telefónicos de estas tomas. Para llamar a alguien necesitamos saber la dirección de SAP de quien debe recibir la llamada.

Para que dos capas intercambien información, tiene que haber un acuerdo sobre el conjunto de reglas relativas a la interfaz. En una interfaz tipica, la entidad de la capa n+1 pasa una IDU (Interface Data Unit, unidad de datos de la interfaz) a la entidad de la capa n a través de SAP.

La IDU consiste en una SDU (Service Data Unit, unidad de datos de servicio) y cierta información de control ICI (Información de Control de la Interfaz). La SDU son los datos necesarios para que las entidades n puedan realizar las funciones pedidas y así dar servicio al nivel n+1. La información de control (ICI) es la información transferida para controlar la interferencia entre dos entidades, pero no forma parte de los datos mismos.

La información intercambiada entre dos entidades n utilizando una comunicación n para realizar las funciones pedidas, toma el nombre de ICI (Información del Control del Protocolo).



Para que se transfiera la SDU, la entidad de la capa n puede tener que fragmentarla en varios pedazos, a cada uno de los cuales se le da un encabezado y se envía como una PDU (Protocol Data Unit, unidad de datos de protocolo) independiente, que podría ser un paquete. Las

entidades pares usan los encabezados de las PDU para acarrear su protocolo de par. Los encabezados indican qué PDU contienen datos y cuáles contienen información de control, proveen números de secuencia y cuentas, etc.

Un servicio se especifica de manera formal con un conjunto de operaciones primitivas disponibles para que un usuario u otra entidad accedan al servicio. Estas primitivas ordenan al servicio que ejecute alguna acción o que informe de una acción que haya tomado una entidad par. Una forma de clasificar las primitivas de servicio es dividirlas en cuatro clases:

- Petición: se utiliza para invocar algún servicio y pasar los parámetros necesarios para especificar el servicio solicitado.
- Indicación: se utiliza para indicar que ha sido invocado un procedimiento por el usuario de servicio en la conexión y para suministrar los parámetros asociados o para notificar al usuario de servicio de una acción iniciada por el suministrador.
- Respuesta: es una función emitida por un usuario de servicio para confirmar o completar algún procedimiento invocado previamente mediante una indicación de ese usuario.
- Confirmación: es una función emitida por un suministrador de servicio para confirmar o completar algún procedimiento invocado previamente mediante una petición por el usuario de servicio.

Las primitivas pueden tener parámetros, y de hecho, la mayor parte de ellas los tiene.

Los parámetros de una petición de conexion pueden especificar la maquina a la que se va a conectar, el tipo de servicio deseado y el tamaño máximo de mensaje a usar en la conexión. Los parámetros de una indicación de conexión podrían contener la identidad de quien llama, el tipo de servicio deseado y el tamaño de mensaje máximo propuesto.

Si la entidad llamada no está de acuerdo con el tamaño máximo propuesto, podría presentar una contrapropuesta en su primitiva de respuesta, que se pondría a disposición del originador de la llamada en la confirmación. Los detalles de esta negociación son parte del protocolo. Por ejemplo, en el caso de dos propuestas en conflicto acerca del tamaño máximo del mensaje, el protocolo podría especificar que siempre se elija el más pequeño.

Hay tres tipos de servicios:

- Servicio con confirmación: Existe una petición, una indicación, una respuesta y una confirmación.
- Servicio no confirmado: Únicamente hay una petición y una indicación.
- Servicio iniciado por el proveedor: Sólo se utiliza la primitiva indicación.

Funcionalidad de cada nivel.

El modelo de referencia OSI está estructurado en siete niveles o capas que cumplen los siguientes requisitos:

- Cada una de las capas desempeña funciones bien definidas.
- Los servicios proporcionados por cada nivel son utilizados por el nivel superior.
- Existe una comunicación virtual entre 2 mismas capas, de manera horizontal.
- Existe una comunicación vertical entre una capa de nivel N y la capa de nivel N + 1.
- La comunicación física se lleva a cabo entre las capas de nivel 1.

NIVEL 1: -CAPA FISICA-. Conexión de equipos.

La capa física abarca el conjunto físico propiamente dicho del que consta toda comunicación y también abarca las reglas por las cuales pasan los bits de uno a otro. Sus principales características son las siguientes:

- Mecánicas: relaciona las propiedades físicas de la interfaz con el medio de transmisión. A veces, incluye la especificación de un conector que une una o más señales del conductor, llamadas circuitos.
- Eléctricas: relaciona la representación de los bits (por ejemplo, en términos de niveles de tensión) y la tasa de transmisión de datos. Maneja voltajes y pulsos eléctricos.
- Funcional: especifica las funciones realizadas por los circuitos individuales de la interfaz física entre un sistema y el medio de transmisión.
- De procedimiento: especifica la secuencia de eventos por los que se intercambia un flujo de bits a través del medio físico.
- Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter, por ejemplo RS-232 y RS-449.

NIVEL 2: -CAPA ENLACE DE DATOS- Detección de errores

Mientras la capa física proporciona solamente un servicio bruto de flujo de datos, la de enlace de datos intenta hacer el enlace físico seguro y proporciona medios para activar, tener y desactivar el enlace. El principal servicio proporcionado por la capa de enlace de datos a las superiores es el de detección de errores y control. Así con un protocolo de la capa de enlace de datos completamente operacional, la capa adyacente superior puede suponer transmisión libre de errores en el enlace.

Sin embargo, si la comunicación es entre dos sistemas que no están directamente conectados, la conexión constará de varios enlaces de datos unidos, cada uno operando independientemente. De este modo no se libera a la capa superior de la responsabilidad del control de errores.

El nivel 2, enlace de datos, provee intercambio de datos entre los dispositivos del mismo medio:

- Detección y control de errores.
- Control de secuencia.
- Control de flujo.
- Control de enlace lógico.
- Control de acceso al medio.
- Sincronización de la trama.

NIVEL 3: -CAPA DE RED-. Encaminamiento.

La capa de red proporciona los medios para la transferencia de información entre los sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de la necesidad de tener conocimiento sobre la transmisión de datos subyacente y las tecnologías de conmutación utilizadas para conectar los sistemas. En esta capa, está envuelto en un diálogo con la red para especificar la dirección de destino y solicitar ciertas facilidades de la red, como prioridad.

Existe un espectro de posibilidades para que las facilidades de comunicacion intermedias sean gestionadas por la capa de red. En un extremo, existe en enlace punto a punto (from point to point) directo entre las estaciones. En este caso, no existe la necesidad de una capa de red ya que la capa de enlace de datos puede proporcionar las funciones necesarias de gestión del enlace. Lo siguiente puede ser un sistema conectado a traves de una única red, coma una red de conmutacion de circuitos de conmutacion de paquetes.

En el otro extremo, dos sistemas finales podrian desear comunicarse, pero sin estar conectados ni siquiera a la misma red. Pero están conectados a redes que, directa o indirectamente, están conectadas unas a otras. Este caso requiere el uso de alguna técnica de interconexión entre redes.

El nivel 3, capa de red, enruta unidades de informacion.

- Esta capa mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.
- Realiza control de congestion.

NIVEL 4: -CAPA DE TRANSPORTE-. Integridad de los mensajes.

La capa de transporte proporciona un mecanismo para intercambiar datos entre sistemas finales.

El servicio de transporte orientado a conexión asegura que los datos se entregan libres de errores, en secuencia y sin pérdidas o duplicados. La capa de transporte puede estar relacionada con la optimización del uso de los servicios de red y proporcionar una calidad del servido solicitada. Por ejemplo, la entidad de sesión puede especificar tasas de error aceptables, retardo máximo, prioridad y seguridad.

El tamaño y la complejidad del protocolo de transporte dependen de que tan seguras o inseguras sean las redes y sus servicios. De acuerdo a esto, ISO ha creado una familia de 5 estándares de protocolos de transporte, cada uno orientado a los diferentes servicios subyacentes.

El nivel 4, capa de transporte, provee la transmisión de datos confiable de punto a punto.

Acepta los datos del nivel de sesion, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red.

Multiplexaje.

- Regula el control de flujo del trafico de extremo a extremo.
- Reconoce los paquetes duplicados.

NIVEL 5: -CAPA DE SESION-. Diálogos de control.

Las cuatro capas más bajas del modelo OSI proporcionan un medio para el intercambio rápido y seguro de datos. Aunque para muchas aplicaciones este servicio básico es insuficiente. Por lo tanto, se tuvo que mejorar algunos aspectos proporcionando unos mecanismos para controlar el diálogo entre aplicaciones en sistemas finales. En muchos casos, habrá poca o ninguna necesidad de la capa de sesion, pero para algunas aplicaciones, estos servicios se utilizan.

Los servicios clave proporcionados por la capa de sesion incluyen los siguientes puntos:

- Disciplina de Diálogo: esta puede ser simultánea en dos sentidos o fullduplex o alternada en los dos sentidos o semi-duplex.
- Agrupamiento: El flujo de datos se puede marcar para definir grupos de datos. Por ejemplo, una tienda de ventas al por menor esta transmitiendo datos de ventas a una oficina regional, estos se pueden marcar para indicar el final de los datos de ventas de cada departamento. Esto indicaría a la computadora que finalice la cuenta de totales para ese departamento y comience una nueva cuenta para el departamento siguiente.

- Recuperación: La capa de sesión puede proporcionar un mecanismo de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

El nivel 5, capa de sesión, coordina la interacción en la sesión (diálogo) de los usuarios:

- Establecimiento de la conexión de sesión.
- Intercambio de datos.
- Liberación de la conexión de sesión.
- Sincronización de la sesión.
- Administración de la sesión.

NIVEL 6: -CAPA DE PRESENTACION-. Interpretación de datos.

La capa de presentación define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. La capa de presentación define la sintaxis utilizada entre entidades de aplicación y proporciona los medios para la seleccion y las subsecuentes modificaciones de la representación utilizada. Algunos ejemplos de los servicios específicos que se podrían realizar en esa capa son los de compresion y encriptado[1] de datos.

- Se da formato a la información para visualizarla o imprimirla.
- Se interpretan los codigos que estén en los datos (conversión de código).
- Se gestiona la encriptación de datos.
- Se realiza la compresión de datos.

NIVEL 7: -CAPA DE APLICACION-. Datos normalizados.

La capa de aplicación proporciona un medio a los programas de aplicación para que accedan al entorno OSI. Esta capa contiene funciones de administración y generalmente mecanismos útiles para admitir aplicaciones distribuidas. Ademas, se considera que residen en esta capa las aplicaciones de uso general como transferencia de archivos correo electrónico y acceso terminal a computadoras remotos.

- Provee servicios generales relacionados con aplicaciones.

[1] Para mayor detalle ver capítulo IV "Monitoreo de Redes"

- Transferencia de archivos (FTP File Transfer Protocol).
- Intercambio de mensajes (correo electrónico).

3.5 Protocolo TCP/IP

Historia

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinito Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. World Wibe Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés).

Arquitectura TCP/IP

TCP/IP es el protocolo común utilizado por todas las computadoras conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectadas computadoras de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un protocolo único, sino que es en realidad un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos
- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

- Red: Es la interfaz de la red real. TCP/IP no especifica ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

- Físico: Análogo al nivel físico del OSI.

NIVEL DE APLICACIÓN
NIVEL DE TRANSPORTE
NIVEL DE INTERNET
NIVEL DE RED
NIVEL FÍSICO

Arquitectura TCP/IP

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP.

Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, esta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

PROTOCOLOS TCP/IP

FTP, SMTP, TELNET	SNMP, X-WINDOWS, RPC, NFS
TCP	UDP
IP, ICMP, 802.2, X.25	
ETHERNET, IEEE 802.2, X.25	

- FTP (File Transfer Protocol). Se utiliza para transferencia de archivos.

- SMTP (Simple Mail Transfer Protocol). Es una aplicación para el correo electrónico
- TELNET: Permite la conexión a una aplicación remota desde un proceso o terminal.
- RPC (Remote Procedure Call). Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- SNMP (Simple Network Management Protocol). Se trata de una aplicación para el control de la red.
- NFS (Network File System). Permite la utilización de archivos distribuidos por los programas de la red.
- X-Windows. Es un protocolo para el manejo de ventanas e interfaces de usuario.

Características de TCP/IP

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen IP mueve los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.

Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino.

Compare esto con la manera en que se transmite una conversación telefónica. Una vez que establece una conexión, se reservan algunos circuitos para usted, que no puede emplear en otra llamada, aun si deja esperando a su interlocutor por veinte minutos.

Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino. Este, claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos computadoras aunque no estén conectadas directamente entre sí. Lo que realmente sorprende es que sólo se necesitan algunos segundos para enviar un archivo de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje.

Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que este disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro.

Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye.

En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

Funcionamiento de TCP/IP

IP

IP a diferencia del protocolo X.25, que está orientado a conexión, es sin conexión. Está basado en la idea de los datagramas interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde la fuente hasta el destinatario, quizás recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera: la capa de transporte toma los mensajes y los divide en datagramas, de hasta 64K octetos cada uno. Cada datagrama se transmite a través de la red red, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un datagrama IP consta de una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable. El formato de la cabecera contiene:

- El campo Version indica a qué versión del protocolo pertenece cada uno de los datagramas. Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.

- El campo Opciones se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Esto, básicamente, proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar, la asignación de bits de cabecera a información que muy rara vez se necesita.

Debido a que la longitud de la cabecera no es constante, un campo de la cabecera, IHL, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. Tamaño 4 bit.

- El campo Tipo de servicio le permite a la fuente indicarle a la subred el tipo de servicio que desea.

Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión.

En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable que entrega rápida. También, es posible tener algunas otras combinaciones, desde un tráfico rutinario, hasta una anulación instantánea. Tamaño 8 bit.

La Longitud total incluye todo lo que se encuentra en el datagrama, tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos (bytes). Tamaño 16 bit.

- El campo Identificación se necesita para permitir que el host destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación. Tamaño 16 bits.

Enseguida viene un bit que no se utiliza, y después dos campos de 1 bit. Las letras **DF** quieren decir no fragmentar. Esta es una orden para que los gateways no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente. Por ejemplo, supóngase que se tiene un datagrama que se carga en un micro pequeño para su ejecución; podría marcarse con DF porque la ROM de micro espera el programa completo en un datagrama. Si el datagrama no puede pasarse a través de una red, se deberá encaminar sobre otra red, o bien, desecharse.

Las letras **MF** significan mas fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificacion doble contra el campo de Longitud total, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

- El desplazamiento de fragmento indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un multiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo Longitud total. Tamaño 16 bits.

- El campo Tiempo de vida es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiendose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits.

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitara saber qué hacer con él. El campo Protocolo indica, a qué proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más.

- Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.

- El código de redundancia de la cabecera es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del código de redundancia de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. Tamaño: 16 bits.

- La Dirección de origen contiene la dirección del host que envía el paquete. Tamaño: 32 bits.

- La Dirección de destino: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bits.

La dirección de Internet

El protocolo IP identifica a cada computadora que se encuentre conectada a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto a la computadora en concreto como la red a la que pertenece, de manera que sea posible distinguir a las computadoras que se encuentran conectadas a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de computadoras en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPANET es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

- Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos

primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del *host* permitiendo, por consiguiente, un número máximo de 64516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de computadoras que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

- Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadoras en cada red.

Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Tabla de direcciones IP de Internet.

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1.. 126	1 byte	3 byte	126	16.387.064
B	128.. 191	2 byte	2 byte	16.256	64.516
C	192.. 223	3 byte	1 byte	2.064.512	254

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de host para máquinas que aún no conocen su número de host dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo

datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de una computadora a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible. En ARPANET y en las líneas punto a punto no es posible enviar broadcast, pero sí que es posible hacerlo en las redes Ethernet, donde se supone que todas las computadoras prestarán atención a este tipo de mensajes.

En el caso de algunas organizaciones extensas puede surgir la necesidad de dividir la red en otras redes más pequeñas (subnets). Como ejemplo podemos suponer una red de clase B que, naturalmente, tiene asignado como identificador de red un número de dos bytes. En este caso sería posible utilizar el tercer byte para indicar en qué red Ethernet se encuentra un host en concreto.

Esta división no tendrá ningún significado para cualquier otra computadora que esté conectada a una red perteneciente a otra organización, puesto que el tercer byte no será comprobado ni tratado de forma especial. Sin embargo, en el interior de esta red existirá una división y será necesario disponer de un software de red especialmente diseñado para ello. De esta forma queda oculta la organización interior de la red, siendo mucho más cómodo el acceso que si se tratara de varias direcciones de clase C independientes.

TCP

Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grande procedentes de los procesos de usuario, los separa en pedazos que no excedan de 64K octetos y, transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden; y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta

Cada octeto de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecidos, desde hace tiempo, en el momento en que los números de secuencia den la vuelta. TCP, sin embargo, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

La primera cosa que llama la atención es que la cabecera mínima de TCP sea de 20 octetos. A diferencia de la clase 4 del modelo OSI, con la cual se puede comparar a grandes rasgos, TCP sólo tiene un formato de cabecera de TPDU (llamadas mensajes). Enseguida se analizará minuciosamente campo por campo, esta gran cabecera. Los campos Puerto fuente y Puerto destino identifican los puntos terminales de la conexión (las direcciones TSAP de acuerdo con la terminología del modelo OSI).Cada hostal deberá decidir por sí mismo como asignar sus puertos.

Los campos Número de secuencia y Asentimiento en superposición efectúan sus funciones usuales. Estos tienen una longitud de 32 bits, debido a que cada octeto de datos está numerado en TCP.

La Longitud de la cabecera TCP indica el número de palabra de 32 bits que están contenidas en la cabecera de TCP. Esta información es necesaria porque el campo Opciones tiene una longitud variable, y por lo tanto la cabecera también.

Después aparecen seis banderas de 1 bit. Si el Puntero acelerado se está utilizando, entonces URG se coloca a 1. El puntero acelerado se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción. El bit SYN se utiliza para el establecimiento de conexiones. La solicitud de conexión tiene SYN=1 y ACK=0, para indicar que el campo de asentimiento en superposición no se está utilizando. La respuesta a la solicitud de conexión sí lleva un asentimiento, por lo que tiene SYN=1 y ACK=1. En esencia, el bit SYN se utiliza para denotar las TPDU connection request y connection confirm, con el bit ACK utilizado para distinguir entre estas dos posibilidades. El bit FIN se utiliza para liberar la conexión; especifica que el emisor ya no tiene más datos. Después de cerrar una conexión, un proceso puede seguir recibiendo datos indefinidamente. El bit RST se utiliza para reiniciar una conexión que se ha vuelto confusa debido a SYN duplicados y retardados, o a caída de los hostales. El bit EOM indica el Fin del Mensaje.

El control de flujo en TCP se trata mediante el uso de una ventana deslizante de tamaño variable.

Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto asentido por el campo ventana y no cuántas TPDU.

El código de redundancia también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits, y después tomar el complemento a 1 de la suma.

El campo de Opciones se utiliza para diferentes cosas, por ejemplo para comunicar tamaño de tampones durante el procedimiento de establecimiento.

En que se utiliza TCP/IP

Muchas grandes redes han sido implementadas con estos protocolos, incluyendo DARPA Internet "Defense Advanced Research Projects Agency Internet", en español, Red de la Agencia de Investigación de Proyectos Avanzados de Defensa. De igual forma, una gran variedad de universidades, agencias gubernamentales y empresas de computadoras, están conectadas mediante los protocolos TCP/IP. Cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes en una red virtual llamada Internet. Las máquinas en Internet son denominadas "hosts" o nodos.

TCP/IP proporciona la base para muchos servicios útiles, incluyendo correo electrónico, transferencia de archivos y login remoto.

El correo electrónico está diseñado para transmitir archivos de texto pequeños. Las utilidades de transferencia sirven para transferir archivos muy grandes que contengan programas o datos.

También pueden proporcionar chequeos de seguridad controlando las transferencias.

El login remoto permite a los usuarios de una computadora acceder a una máquina remota y llevar a cabo una sesión interactiva.

Similitudes y Diferencias entre la clase 4 del Modelo OSI y TCP

El protocolo de transporte de clase 4 del modelo OSI (al que con frecuencia se le llama TP4), y TCP tienen numerosas similitudes, pero también algunas diferencias. A continuación se dan a conocer los puntos en que los dos protocolos son iguales. Los dos protocolos están diseñados para proporcionar un servicio de transporte seguro, orientado a conexión y de extremo a extremo, sobre una red insegura, que puede perder, dañar, almacenar y duplicar paquetes. Los dos deben enfrentarse a los peores problemas como sería el caso de una subred que pudiera almacenar una secuencia válida de paquetes y más tarde volviera a entregarlos.

Los dos protocolos también son semejantes por el hecho de que los dos tienen una fase de establecimiento de conexión, una fase de transferencia de datos y después una fase de liberación de la conexión. Los conceptos generales del establecimiento, uso y liberación de conexiones también son similares, aunque difieren en algunos detalles. En particular, tanto TP4 como TCP utilizan la comunicación ida-vuelta-ida para eliminar las dificultades potenciales ocasionadas por paquetes antiguos que aparecieran súbitamente y pudiesen causar problemas.

Sin embargo, los dos protocolos también presentan diferencias muy notables, las cuales se pueden observar en la lista que se muestra en la figura siguiente. Primero, TP4 utiliza nueve tipos diferentes de TPDU, en tanto que TCP solo tiene uno. Esta diferencia trae como resultado que TCP sea más sencillo, pero al mismo tiempo también necesita una cabecera mas grande, porque todos los campos deben estar presentes en todas las TPDU. El mínimo tamaño de la cabecera TCP es de 20 octetos; el mínimo tamaño de la cabecera TP4 es de 5 octetos. Los dos protocolos permiten campos opcionales, que pueden incrementar el tamaño de las cabeceras por encima del mínimo permitido.

CARACTERÍSTICA	OSI TP4	TCP
Número de tipos de TPDU	9	1
Fallo de Conexión	2 conexiones	1 conexión
Formato de direcciones	No está definido	32 bits
Calidad de servicio	Extremo abierto	Opciones específicas
Datos del usuario en CR	Permitido	No permitido
Flujo	Mensajes	Octetos
Datos importantes	Acelerados	Acelerados
Superposición	No	Sí
Control de flujo explícito	Algunas veces	Siempre
Número de subsecuencia	Permitidos	No Permitido
Liberación	Abrupta	Ordenada

Diferencias entre el protocolo TP4 del modelo OSI y TCP

Una segunda diferencia es con respecto a lo que sucede cuando los dos procesos, en forma simultánea, intentan establecer conexiones entre los mismos dos TSAP (es decir, una colisión de conexiones). Con TP4 se establecen dos conexiones duplex independientes; en tanto que con TCP, una conexión se identifica mediante un par de TSAP, por lo que solamente se establece una conexión.

Una tercera diferencia es con respecto al formato de direcciones que se utiliza. TP4 no especifica el formato exacto de una dirección TSAP; mientras que TCP utiliza números de 32 bits.

El concepto de calidad de servicio también se trata en forma diferente en los dos protocolos, constituyendo la cuarta diferencia. TP4 tiene un mecanismo de extremo abierto, bastante elaborado, para una negociación a tres bandas sobre la calidad de servicio. Esta negociación incluye al proceso que hace la llamada, al proceso que es llamado y al mismo servicio de transporte. Se pueden especificar muchos parámetros, y pueden proporcionarse los valores: deseado y mínimo aceptable. A diferencia de esto, TCP no tiene ningún campo de calidad de servicio, sino que el servicio subyacente IP tiene un campo de 8 bits, el cual permite que se haga una relación a partir de un número limitado de combinaciones de velocidad y seguridad.

Una quinta diferencia es que TP4 permite que los datos del usuario sean transportados en la TPDU CR, pero TCP no permite que los datos del usuario aparezcan en la TPDU inicial. El dato inicial (como por ejemplo, una contraseña), podría ser necesario para decidir si se debe, o no, establecer una conexión. Con TCP no es posible hacer que el establecimiento dependa de los datos del usuario.

Las cuatro diferencias anteriores se relacionan con la fase de establecimiento de la conexión. Las cinco siguientes se relacionan con la fase de transferencia de datos. Una diferencia básica

es el modelo del transporte de datos. El modelo TP4 es el de una serie de mensajes ordenados (correspondientes a las TSDU en la terminología OSI).

El modelo TCP es el de un flujo continuo de octetos, sin que haya ningún límite explícito entre mensajes. En la práctica, sin embargo, el modelo TCP no es realmente un flujo puro de octetos, porque el procedimiento de biblioteca denominado push puede llamarse para sacar todos los datos que estén almacenados, pero que todavía no se hayan transmitido. Cuando el usuario remoto lleva a cabo una operación de lectura, los datos anteriores y posteriores al push no se combinarán, por lo que, en cierta forma un push podría penarse como si definiesen una frontera entre mensajes.

La séptima diferencia se ocupa de como son tratados los datos importantes que necesitan de un procesamiento especial (como los caracteres BREAK). TP4 tiene dos flujos de mensajes independientes, los datos normales y los acelerados multiplexados de manera conjunta. En cualquier instante únicamente un mensaje acelerado puede estar activo.

TCP utiliza el campo Acelerado para indicar que cierta cantidad de octetos, dentro de la TPDU actualmente en uso, es especial y debería procesarse fuera de orden.

La octava diferencia es la ausencia del concepto de superposición en TP4 y su presencia en TCP.

Esta diferencia no es tan significativa como al principio podría parecer, dado que es posible que una entidad de transporte ponga dos TPDU, por ejemplo, DT y AK en un único paquete de red.

La novena diferencia se relaciona con la forma como se trata el control de flujo. TP4 puede utilizar un esquema de crédito, pero también se puede basar en el esquema de ventana de la capa de red para regular el flujo. TCP siempre utiliza un mecanismo de control de flujo explícito con el tamaño de la ventana especificado en cada TPDU.

La décima diferencia se relaciona con este esquema de ventana. En ambos protocolos el receptor tiene la capacidad de reducir la ventana en forma voluntaria. Esta posibilidad genera potencialmente problemas, si el otorgamiento de una ventana grande y su contracción subsiguiente llegan en un orden incorrecto. En TCP no hay ninguna solución para este problema; en tanto en TP4 este se resuelve por medio del número de subsecuencia que está incluido en la contracción, permitiendo de esta manera que el emisor determine si la ventana pequeña siguió, o precedió, a la más grande.

Finalmente, la onceava y última diferencia existente entre los dos protocolos, consiste en la manera como se liberan las conexiones. TP4 utiliza una desconexión abrupta en la que una serie de TPDU de datos pueden ser seguidos directamente por una TPDU DR. Si las TPDU de datos se llegaran a perder, el protocolo no los podría recuperar y la información, al final se perdería. TCP utiliza una comunicación de ida-vuelta-ida para evitar la pérdida de datos en el momento de la desconexión. El modelo OSI trata este problema en la capa de sesión. Es importante hacer notar que la Oficina Nacional de Normalización de Estados Unidos estaba tan disgustada con esta propiedad de TP4, que introdujo TPDU adicionales en el protocolo de

transporte para permitir la desconexión sin que hubiera una pérdida de datos. Como consecuencia de esto, las versiones de Estados Unidos y la internacional de TP4 son diferentes.

Es importante señalar que el protocolo IP explicado anteriormente, o mejor dicho la versión de éste es la más utilizada actualmente, pero hace muy poco tiempo salió una nueva versión llamada la número 6. Las diferencias no son muchas, pero mejoran muchos aspectos de la antigua, ésta no es muy utilizada, pero creemos que es necesario explicar como funciona, para poder hacer una comparación con la antigua. A continuación la trataremos.

La nueva versión de IP (IPng)

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (Internet Protocol Next Generation). El número de versión de este protocolo es el 6 (que es utilizada en forma mínima) frente a la antigua versión utilizada en forma mayoritaria. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.).

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas.

Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

Formato de la cabecera.

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior.

Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión. El formato completo de la cabecera sin las extensiones es el siguiente:

- Versión: Número de versión del protocolo IP, que en este caso contendrá el valor 6. Tamaño: 4 bit.
- Prioridad: Contiene el valor de la prioridad o importancia del paquete que se esta enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 4 bit.

- Etiqueta de flujo: Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los routers que lo soporten. Tamaño: 24 bit.

- Longitud: Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 bit.

- Siguiente cabecera: Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 bit.

- Límite de existencia: Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño: 8 bit.

- Dirección de origen: El número de dirección del host que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 bit.

- Dirección de destino: Número de dirección de destino, aunque puede no coincidir con la dirección del host final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. Tamaño: 128 bit.

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no esta limitado a un valor fijo de bytes como ocurria en la versión 4.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para routing extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

Direcciones en la versión 6.

El sistema de direcciones es uno de los cambios mas importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bit (cuatro veces mayor). Estas nuevas direcciones identifican a una interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos a traves de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme.

Teóricamente serian 2^{128} direcciones posibles, siempre que no apliquemos algún formato u organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 trillones de direcciones distintas por cada metro cuadrado de la superficie del planeta Tierra.

Según diversas fuentes consultadas, estos números una vez organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564 direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a una interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso. Estos tres tipos de direcciones son:

- Direcciones unicast: Son las direcciones dirigidas a un único interfaz de la red. Las direcciones unicast que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.

- Direcciones anycast: Identifican a un conjunto de interfaces de la red. El paquete se enviará a una interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones unicast que se encuentran asignadas a varias interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones unicast.

- Direcciones multicast: Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente.

Las direcciones de broadcast no están implementadas en esta versión del protocolo, debido a que esta misma función puede realizarse ahora mediante el uso de las direcciones multicast.

Características de IPv6

A continuación se enumeran las características del nuevo protocolo IPv6:

- Nuevo formato de encabezado
- Gran espacio de direcciones
- Direccionamiento jerárquico e infraestructura de enrutamiento eficientes
- Configuración de direcciones sin estado y con estado
- Seguridad integrada
- Mayor compatibilidad con QoS
- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

Nuevo formato de encabezado

El encabezado de IPv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima. Para ello, se mueven los campos de opciones y los que no son esenciales a encabezados de extensión que se colocan tras el encabezado de IPv6. El encabezado optimizado de IPv6 proporciona un procesamiento más eficiente en los enrutadores intermedios.

Los encabezados de IPv4 no pueden funcionar conjuntamente con los encabezados de IPv6. Un host o un enrutador deben utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado de IPv6 es sólo el doble de grande que el de IPv4, aunque las direcciones de IPv6 son cuatro veces mayores que las de IPv4.

Gran espacio de direcciones

IPv6 tiene direcciones IP de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden expresar más de $3,4x10^{38}$ combinaciones posibles, el gran espacio de direcciones de IPv6 se ha diseñado para permitir varios niveles de subredes y asignaciones de redes de la red troncal de Internet a las subredes individuales de una organización.

Aunque actualmente sólo se asigna un pequeño número de las direcciones posibles para los hosts, hay muchas direcciones disponibles para su uso en el futuro. Con un número de direcciones disponibles mucho mayor, dejan de ser necesarias las técnicas de conservación de direcciones, como la distribución de NAT.

Direccionamiento jerárquico e infraestructura de enrutamiento eficientes

Las direcciones globales de IPv6 utilizadas en la parte IPv6 de Internet están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios Internet. En Internet IPv6, los enrutadores troncales tienen tablas de enrutamiento mucho más pequeñas, que corresponden a la infraestructura de enrutamiento de Agregadores de nivel superior.

Configuración de direcciones sin estado y con estado

Para simplificar la configuración de hosts, IPv6 permite la configuración de direcciones con estado, (como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado, configuración de direcciones en ausencia de un servidor DHCP). Con una configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (que se denominan direcciones locales de vínculo) y con direcciones derivadas de prefijos anunciados por enrutadores locales. Incluso en ausencia de un enrutador, los hosts del mismo vínculo pueden configurarse automáticamente con direcciones locales de vínculo y se comunican sin configuración manual

Seguridad integrada

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6.

Mayor compatibilidad con QoS

Los nuevos campos del encabezado de IPv6 definen cómo se identifica y se controla el tráfico. La identificación del tráfico mediante un campo Flow Label (Etiqueta de flujo) en el encabezado de IPv6 permite a los enrutadores identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo, un conjunto de paquetes que viaja entre un origen y un destino. Como el tráfico se identifica en el encabezado de IPv6, se puede proporcionar compatibilidad con QoS incluso si la carga de paquetes está cifrada mediante IPSec.

Nuevo protocolo para la interacción de nodos vecinos

El protocolo Neighbor Discovery (Descubrimiento de vecino) para IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, Internet Control Message Protocol for IPv6) que administran la interacción de nodos vecinos (nodos que se encuentran en el mismo vínculo). Neighbor Discovery reemplaza al Protocolo de resolución de direcciones (ARP, Address Resolution Protocol) basado en difusión, al protocolo de descubrimiento de enrutadores de ICMPv4 y a los mensajes Redirect (Redirección) de ICMPv4 con mensajes Neighbor Discovery de unidifusión y multidifusión.

Capacidad de ampliación

IPv6 se puede ampliar fácilmente con nuevas características si se agregan encabezados de extensión tras el encabezado de IPv6. A diferencia de las opciones del encabezado de IPv4, que sólo permite 40 bytes de opciones, el tamaño de los encabezados de extensión de IPv6 sólo está limitado por el tamaño del paquete de IPv6.

Diferencias entre IP6 e IP4

En la siguiente tabla pueden contemplarse y compararse las diferencias y mejoras de IP6 respecto a IP4

IPv4	IPv6
Las direcciones de origen y de destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y de destino tienen una longitud de 128 bits (16 bytes)
La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria.
No hay identificación de carga para el control de QoS por parte de los enrutadores en el encabezado de IPv4	La identificación de carga para el control de QoS por parte de los enrutadores se incluye en el encabezado de IPv6 mediante el campo Flow Label (Etiqueta de flujo)
La fragmentación es posible en ambos enrutadores y en el host de envío.	La fragmentación no es posible en los enrutadores. Sólo es posible en el host de envío
El encabezado incluye una suma de comprobación	El encabezado no incluye una suma de comprobación
El encabezado incluye opciones	Todos los datos opcionales se mueven a extensiones de encabezado IPv6
El Protocolo de resolución de direcciones (ARP) utiliza tramas de solicitud de ARP de difusión para resolver una dirección de IPv4 en una dirección de nivel de vínculo.	Las tramas de solicitud de ARP se reemplazan por mensajes Neighbor Solicitation (Solicitud de vecino) de multidifusión
Se utiliza el Protocolo de administración de grupos de Internet (IGMP) para administrar la pertenencia a grupos de subredes locales.	El protocolo IGMP se reemplaza por mensajes Multicast Listener Discovery (MLD o Descubrimiento de escucha de multidifusión)
Para determinar la dirección IPv4 de la mejor puerta de enlace predeterminada se utiliza el descubrimiento de enrutadores de ICMP, que es opcional	El descubrimiento de enrutadores de ICMPv4 se reemplaza por los mensajes Router Solicitation (Solicitud de enrutador) y Router Advertisement (Anuncio de enrutador) de ICMPv6, que son necesarios
Las direcciones de difusión se utilizan para enviar tráfico a todos los nodos de una subred	No hay direcciones de difusión de IPv6. En su lugar, se utiliza una dirección de multidifusión para todos los nodos de ámbito local de vínculo
La configuración debe efectuarse manualmente o a través de DHCP	No se necesita configuración manual ni DHCP
Utiliza registros de recursos (A) de dirección de host en el Sistema de nombres de dominio (DNS, Domain Name System) para asignar nombres de host a direcciones IPv4	Utiliza registros de recursos (AAAA) de dirección de host en el Sistema de nombres de dominio (DNS) para asignar nombres de host a direcciones IPv6
Utiliza registros del recurso Puntero (PTR) en el dominio DNS IN-ADDR.ARPA para asignar direcciones de IPv4 a nombres de host.	Utiliza registros del recurso Puntero (PTR) en el dominio DNS IP6.INT para asignar direcciones de IPv6 a nombres de host

CAPÍTULO IV

MONITOREO DE REDES

CAPITULO IV

MONITOREO DE REDES

4.1 Introducción

El costo del tiempo muerto por deficiencias en las redes y el descontento del cliente son causas muy grandes para la perdida de ingresos en las empresas.

Hoy en día las empresas enfrentan una serie de cambios tecnológicos y competitivos muy fuertes que las llevan inevitablemente a la inversión de herramientas de monitoreo y se han dado cuenta que más que una pérdida en la inversión de estas, es una oportunidad para enfrentar a sus competidores.

Es entonces, cuando se hacen la pregunta ¿Como me doy cuenta del estado actual de mi red? y la respuesta está, en los mecanismos de auditoria, los cuales integran al monitoreo que no es otra cosa que la revisión formal (vigilancia) de los resultados arrojados por la supervisión de un Sistema. Algunos mecanismos de Auditoria son:

- Las Bitácoras del Sistema Operativo y del Firewall.
- Los Detectores de Intrusos basados en host y en red.
- Los Analizadores de Estado como los Scripts de Ping y las consolas basadas en SNMP.

El desarrollo de distintas herramientas y necesidades de monitoreo, ha llevado a la clasificación de dos tipos de monitoreo, Monitoreo Funcional y el Monitoreo de Seguridad.

Monitoreo Funcional: es el encargado de verificar la disponibilidad de los dispositivos conectados a la red que permiten que las Aplicaciones lleguen al usuario final sin ningún problema, por ejemplo, si un equipo esta activo, debe responder al ping; si un proceso está ejecutándose aparece en el listado de procesos activos, si un usuario esta firmado, se muestra en el listado de usuarios activos, etc.

En otras palabras el monitoreo funcional es el encargado de verificar la actividad del Sistema, su desempeño, las operaciones transaccionales y de cuidar la disponibilidad de nuestro Sistema.

Monitoreo de Seguridad: se encarga de verificar la integridad y confidencialidad del proceso, la fuente, el destino, así como mantener el ambiente bajo un perímetro para evitar fugas o inserciones.

Cabe resaltar que ambos (Monitoreo Funcional y Seguridad) deben ser considerados como complementarios y no como suplementarios.

Consideraciones del Monitoreo de una Red.

Para poder llevar a cabo un monitoreo adecuado en la red, será necesario instalar software y hardware, es muy importante que al elegirlo analicemos los requerimientos del mismo y los que la red posee, de tal manera que no se afecte el desempeño.
Algunos aspectos a verificar son:

- Determinar que es lo que realmente se requiere vigilar, tomando en cuenta que por cada elemento adicional que se desee monitorear, implicará un costo de administración adicional.
- El proceso de Monitoreo será automático o manual, en otras palabras se dispone de personal entrenado para realizar la función o se confía en que el calendario de tareas va a realizar siempre su trabajo.
- La plataforma a implementar es lo suficientemente robusta, es decir, se puede integrar con otras consolas de monitoreo para no estar sujeta a una sola.
- Que pueda descubrir diversos dispositivos (de Voz, Datos, Frame Relay, ATM, PBX, PC's, Servers) y de diferentes marcas.
- Número de usuarios que accesan a la red.
- La velocidad y tecnología de la red.
- Que dicho software pueda manejar el servicio de SNMP, para obtener mejores resultados de los dispositivos monitoreados.
- Que tenga un ambiente fácil de manejar y que los resultados puedan visualizarse en pocas ventanas.
- Que pueda contar con reporteador y con estadísticas, para poder sacar la información de su misma base de datos del software de monitoreo, o bien se pueda exportar la información a otra base de datos.
- Es importante contar con un software que nos de una "capacidad de planeación" para detectar a corto, mediano y a largo plazo la capacidad de los dispositivos conectados a la red.
- Establecer umbrales de acuerdo al comportamiento y estado crítico.
- Los recursos que consume la aplicación de monitoreo.
- Configuración de las terminales.

- Configuración y versiones de los protocolos.
- Revisar si los protocolos se encuentran actualizados.
- El estado de los ruteadores y si se encuentran actualizados.
- Designación de los puertos de la aplicación.
- Revisar si las direcciones IP de las máquinas se encuentran asignadas.
- Tiempos de acceso requeridos (óptimos) de acuerdo a las características específicas de la red.
- Los mecanismos de control de flujo.
- Prioridades de los servicios.
- Tamaño de la red (segmentaciones, puentes, Intranets, etc.).
- Revisión del cableado, es decir, si soporta las aplicaciones que corren (ancho de banda).
- Revisar si los conectores se encuentran en buen estado.
- Revisar la fuente de poder.

4.2 Monitoreo Funcional

La labor de administración de las redes ha cobrado mayor importancia hoy día. Con el crecimiento de Internet, las redes han aumentado en tamaño, complejidad, ancho de banda, necesidades de usuarios y tecnologías y sus configuraciones están cambiando constantemente, exigiendo, cada vez más recursos y personal necesarios para su gestión. Ahora, más que nunca son esenciales, las herramientas y servicios automatizados que ayuden a prevenir, encontrar y ajustar los problemas de la red.

Estas herramientas deben tener la capacidad de:

- Optimizar el rendimiento y fiabilidad.
- Diagnosticar y prevenir problemas.
- Administrar proactivamete
- Calcular tendencias y generar reportes.

Monitoreo de Recursos y Herramientas

Se recomienda monitorear los siguientes elementos:

Cache
Monitorear los archivos de memoria y su actividad. Esto permite asegurar la disponibilidad de espacio en el cache lo que repercute en la velocidad de procesamiento

CPU
Monitorear el uso y la actividad del CPU, a través de un número de interrupciones del dispositivo. Mediante los resultados obtenidos puede determinarse los procesadores con más carga de trabajo así como la necesidad de renovarlos.

Event Logs
Es conveniente monitorear las divisiones flexibles del sistema, seguridad y aplicaciones de event logs por evento, con una notificación inmediata o periódica, alarma manual o alarma vía otro agente.

Discos Lógicos
Monitorear y garantizar la disponibilidad de un recurso de archivo de sistema de datos asegurando una proporción de espacio libre en la unidad de disco lógico con respecto al total de espacio disponible a usar.

Memorias
Desplegar estadísticas de memoria a manera de bytes disponibles y medida de memoria usada y no usada.

Red
Monitorear la actividad de la red y proveer información acerca de la velocidad a la cual los bytes y paquetes son recibidos o enviados sobre una conexión TCP/IP.

Discos Físicos
Monitorear los recursos de los discos físicos para vigilar su correcto funcionamiento para preservar la integridad de la información.

Impresoras
Monitorear impresoras y proveer información como nombre de impresora, nombre del puerto, número de trabajos y estatus para distribuir la carga de trabajo.

Procesos
Monitorear procesos, usos de memoria virtual y umbrales de funcionamiento, desplegando y registrando los procesos de los CPU s más usados.

Protocolo
Monitorear la carga de protocolos en la red para eliminar los protocolos innecesarios

Registro
Monitorear el porcentaje del contador de registros a ser usados. Informando el valor actual del registro y cuando debe cambiar.

Seguridad
Monitorear la red y la seguridad del servidor a manera de chequeo del número de veces fallidas que se intenta abrir un archivo por no estar autorizado.

Servidor
Monitorear los servicios del servidor para asegurar la disponibilidad de los recursos.

Servicios
Disparar alarmas o advertir dependiendo del estado o duración de los servicios.

Sistema
Monitorear el estado de los objetos del sistema operativo y asegurar que la capacidad del sistema es suficiente para la demanda.

Monitoreo del Dominio
Proveer al administrador de la red la capacidad de entender como muchas estaciones de trabajo, servidores, controladores y usuarios de sesiones están actualmente usando el dominio de la red. El administrador puede elegir límites que se podrán levantar en un evento cuando el número o nodos indican un problema. Monitoreando el numero de computadoras que están conectadas al dominio permite al usuario obtener información histórica que se usa para planear la capacidad de la red al mismo tiempo que recibe alarmas cuando las computadoras criticas no se encuentran ya en línea.

DHCP (Dinamic Host Configuration Protocol)
Administrar los servicios del servidor DHCP que puedan estar corriendo. Incluye variables como velocidad requerida y la velocidad liberada. Los servidores de DHCP son la herramienta para administrar direcciones IP en un ambiente determinado

DNS (Domain Name System)
En cualquier momento una computadora tiene acceso al host TCP/IP, el nombre de una resolución debe ocurrir para resolver los nombre de los textos de Internet dentro de la dirección IP. Esencialmente si el servicio DNS no esta trabajando apropiadamente, los usuarios finales no pueden conectarse al host de Internet. El valor es para reducir el bajo tiempo de conectividad TCP/IP junto con los problemas DNS

RAS (Remote Access Server)
Proveer a los usuarios de la red la capacidad de firmarse en el ambiente remotamente vía un teléfono o una conexión ISDN. Si los dispositivos RAS no están funcionando apropiadamente será difícil si no es que imposible para los usuarios remotos ingresar, por lo tanto, se recomienda monitorear el estatus de cada acceso remoto que exista dentro del dominio.

Usuarios
Monitorear los recursos usados por cuentas individuales dentro del dominio para analizar la capacidad utilizada así como la seguridad dentro del sistema. Mediante el análisis de los resultados puede planearse la evolución del sistema.

4.2.1) Software Comercial

Analizadores de Protocolos

Los analizadores de protocolos son dispositivos que colaboran en la tarea de monitorear el comportamiento de las redes o enlaces de datos, para que la productividad de una entidad no se deteriore por fallas o anomalías de dichos sistemas.

El analizador de protocolo permite escudriñar el interior de las redes y saber que está pasando en cada momento, a nivel de conceptos, como tráfico y congestión, que son los mayores provocadores de los problemas de la red y que sin un equipo de medición adecuado, son muy difíciles de detectar.

Algunos de los analizadores que actualmente están en el mercado son:

WIRESPEED.
Es una herramienta para redes ATM 622 Mbps. Corre en una plataforma Windows NT, que permite la solución de los problemas eficazmente y realiza mantenimiento preventivo.

DS-300/DS-500.
Ofrece análisis de protocolo, simulación, prueba y emula terminales para todos los protocolos comunes.

ISDN 1000PA.
El software corre bajo la plataforma Windows. Se conecta en serie con la interfaz de usuario.

PARASCOPE 2000.
Realiza supervisiones físicas, análisis protocolar, analisis estadístico, proporción de errores y simulación en líneas de comunicación de datos.

DA-320 Dominon LAN Analizador Interred
Descifra más de 300 protocolos, posee autoconfiguración, fácil de usar con una interfaz para Windows.

DOMINOLAN
Puede descifrar todos los protocolos y monitorear el tráfico de la red en Ethernet y Token Ring.

LANDECODER32.
Diseñado para Windows 95 y Windows NT 4.0 El software puede operar en redes de distinta topología Posee ayuda en línea.

MODEL 903. PC COMCOPE II PROTOCOL ANALYZER.
Puede ejecutarse un número ilimitado de veces permitiendo tener varias ventanas independientes actualizándose en tiempo real.

SONDA.
Para equipos portátiles, aporta una solución completa a las redes de área extendida (WAN)

WEBTRENDS

- Webtrends para "firewalls" y "vpns" v. 1.0
  Administración en tiempo real, reportes y monitoreo corporativo de firewalls.

- WebTrends Suite para "Lotus Domino"
  Administracion, reportes y analisis de Servidores Web en Lotus Domino.

A continuación presentaremos algunos softwares utilizados para el monitoreo funcional de una red:

PACKETSHAPER
Packeteer ofrece tres productos para WAN:

- PacketShaper 1000 maneja conexiones a 384 Kbps en LAN's a 10 Mbps.

- PacketShaper 2000 maneja velocidades de 10 Mbps en LAN's a 10 Mbps.

- PacketShaper 4000 maneja velocidades a 45 Mbps en LAN's a 10 o 100 Mbps.

AIX NETVIEW/6000
Aplicación para gestión de redes TCP/IP. Posee un interfaz gráfico con la capacidad de "arrastrar y soltar". Monitoreo y mapeo dinámico de la red y de sus recursos. Manejo de dispositivos de varios fabricantes

SNMP.
Su principal objetivo es el integrar la gestión de diferentes tipos de redes mediante un diseño sencillo con poca sobrecarga en la red. SNMP opera utilizando el protocolo IP, por lo que ignora los aspectos específicos del hardware sobre el que funciona

OPTIVITY
Este es un sistema de administración de redes. Se caracteriza por incluir administración de fallas, análisis funcional, reportes y acceso al nivel de seguridad. El sistema de administración de red Optivity se basa en una arquitectura cliente/servidor que soporta cualquier sistema operativo actual. Posee una visión potencial y la capacidad de localizar fallas y aislarlas, además ofrece un centro de servicios en base a fallas, topologías y correcciones estadísticas.

Sus aplicaciones son diseñadas para controlar el soporte de un nuevo hardware, ayuda a los administradores de red para incorporar rápidamente un equipo nuevo bajo un solo sistema de administración.

Los administradores de red obtienen una visión general del monitoreo de redes, localización de fallas y administración práctica.

El sistema de administración de red Optivity ofrece:

- Facilidad para usar aplicaciones basados en Java que provee una uniforme visualización a través de interfaces Windows, Web y Unix.
- Un procedimiento apropiado de acceso a usuarios para aplicaciones de seguridad no autorizados.
- Servicios internos que permiten la revisión del nivel del sistema de la red.
- Un sistema inteligente de fallas, la cual provee gráficas de correlación y segregación de fallas.
- La aplicación InfoCenter, la cual permite a los administradores el control de fallas de correlación, registro de red y topología en una subred, segmento, dispositivo o interfaz de ruta.
- La aplicación Path Trace la cual muestra los significados de lo que se está viendo y la localización de fallas.
- La aplicación OmniView, la cual entrega una sofisticada colección de estadísticas que permite que la información sea desplegada en un formato de gráfica o tabulación permitiendo a los clientes el análisis de la red.
- ExpandedView, la cual presenta una interacción, una visualización en tiempo real del dispositivo de red seleccionado y así los administradores pueden monitorear, configurar y recobrar estadísticas.
- La Database Administration Tool, la cual ofrece un rápido y efectivo método de recuperación de aplicaciones críticas y base de datos de usuarios.
- La administración de redes Frame Relay es simplificada mediante una sencilla gráfica disponible y una información estadística.
- También Optivity permite el monitoreo de datos y redes de telefonía. Estos productos pueden ser usados para optimizar una red, detectar problemas rápidamente y arreglar estos problemas antes de que tenga interrupciones. Aunque el mayor provecho se obtiene cuando estas aplicaciones son combinadas para administrar una red como un

sistema integrado. El escoger la aplicación apropiada de Optivity permite a las organizaciones una óptima administración de las redes.

A continuación tenemos algunos ejemplos de estas aplicaciones:

- Optivity Network Management System
  Es un sistema de monitoreo funcional que diagnostica fallas en tiempo real para redes de datos.

- Optivity NetID
  NetID es un fruto del protocolo IP para aplicaciones administrativas que combina diversas características con robustez, estabilidad y accesibilidad.

- Optivity Policy Services
  Es un software de aplicación nivel-sistema designado para proveer prioridades en el entorno de la red de una empresa.

- Optivity Switch Manager
  Es una aplicación de bajo costo para configurar y manejar cambios en una red de datos de una empresa.

- Optivity Telephony Manager para Meridian SL-100
  Es la plataforma designada para sistemas de comunicación.

WHATSUP GOLD

WhatsUp Gold es una solución de mapeado, monitoreo y notificación gráfica para redes, de alto rendimiento y bajo costo, que mantiene la red activa 24 horas al día, siete días a la semana. Es fácil de configurar para un entorno de red concreto, ampliable para monitorear redes de empresa en expansión y simple de administrar.

Posee mapas gráficos de la red, con alarmas locales que ayudan a controlar los problemas de inactividad de la red.

Monitoreo de una amplia variedad de dispositivos y servicios, con protocolos de uso corriente.

Notificación remota, a través de buscapersonas o por correo electrónico

Interfaz de Web interactiva que permite comprobar el estado de los dispositivos de la red y llevar a cabo las tareas administrativas rutinarias a través del Web.

Arquitectura multisubproceso compatible con varios mapas jerárquicos para ayudar a acomodar el crecimiento de la red.

Capacidad para ejecutarse como un servicio de sistema de Windows NT, lo que proporciona seguridad añadida.

Notificaciones de grupo que permiten definir con facilidad "equipos de respuesta" que serán notificados de una condición de alerta.

Monitoreo personalizado de servicios que ayuda a llevar el seguimiento de aplicaciones críticas como Lotus Notes, Oracle, SQL Server, Sybase, Exchange u otras.

TOTAL NETWORK VISIBILITY (TNV)

La suite Total Network Visibility (TNV) se basa en la tecnología Sniffer - incluye el mayor número de decodificaciones de protocolos- y proporciona análisis para localizar y analizar automáticamente los problemas de las redes, recomendando soluciones para su resolución inmediata y prevención futura. Sniffer optimiza el rendimiento y la fiabilidad, corrige y previene problemas, realiza una gestión proactiva, evalúa tendencias y genera informes.

Sniffer TNV está compuesto de las siguientes suites:

- Sniffer Pro Analysis Suite: Funciona en PCs portátiles o en PCs estándar para satisfacer las distintas necesidades de redes. Emplean la mayor colección en la industria de decodificadores de protocolos, más un análisis experto para señalar y analizar automáticamente problemas de redes, y recomendar soluciones para corregirlos ahora y prevenirlos en el futuro.

- Distributed Analysis Suite: abarca desde la cobertura básica hasta redes troncales de comunicación o de misión crítica. Estas suites combinan la capacidad de decodificación y de análisis con estadísticas de nivel de servicio y análisis proactivo de dispositivo. Esta combinación pone en sus manos un poderoso sistema para señalar y analizar automáticamente problemas de redes, que mantiene su red distribuida en los niveles más altos de rendimiento y fiabilidad.

- Network Informant Suite: Esta nueva solución corporativa de reportes basada en una arquitectura distribuida, recolecta datos desde una variedad de recursos de la red y recopila una completa visión del desempeño de la red.

PATROL

Patrol modela los cambios en hardware, aplicaciones y tasas de transacción, tiene la capacidad para modelar soluciones que envuelven múltiples sistemas. Por ejemplo en una aplicación usando un servidor Web Microsoft Windows 2000 y en una aplicación Unix, serán fácilmente modelado usando Patrol. El modelo predecible de Patrol entrega la evaluación del negocio en varias maneras:

- Control de costos a través de la utilización de sistemas optimizados y difiriendo gastos del hardware.

- Asegura el rendimiento con acuerdos entre el nivel del servicio, incrementando el uso y la satisfacción del cliente.

- Incrementa la capacidad de administración del crecimiento de la infraestructura haciendo no necesaria otra fuente de administración adicional.

- Reduce el riesgo de la implementación de un proyecto, acelera el tiempo de evaluación, e improvisa operaciones.

Como sistema distribuido es más complejo, en combinaciones diversas de Unix, Microsoft Windows NT y sistemas de Windows 2000, la habilidad de manejar un ambiente integrado se hace crucial en el éxito comercial.

Porque el sistema, aplicación y la actuación del banco de datos tocan un factor mayor en la efectividad de una compañía, ya que los profesionales de sistemas de información al estar bajo presión incesante logran más con menos recursos.

Al mismo tiempo, el costo y la complejidad de sistemas administrativos, aplicaciones y base de datos seguira creciendo. Ademas, con dependencia elevada en sistemas y aplicaciones aumenta la disponibilidad de demanda en un 100% y el tiempo de respuesta es mejor.

Patrol proporciona la capacidad para comprender cómo las aplicaciones comerciales se están realizando, identificando y resolviendo rápidamente posibles fallas en la aplicación.

Si se cuenta con sistemas de Unix, Windows 2000 o ambos, Patrol encontrará todo sobre su administración funcional y la planeación necesaria para su desarrollo.
Basado en fundamentos esenciales de exactitud, almacenamiento de datos eficientes y operaciones simplificadas, Patrol para Unix-funcional adiciona la manera de administración funcional en una empresa distribuida.

Los productos funcionales de Patrol son construidos sobre una metodología de colección "todo el dato, todo el tiempo". La razón es asegurar datos funcionales por completo, para analizar, reportar y predecir los datos exactos.

El proceso de colección de datos funcionales de Patrol es totalmente automatizado, eliminando la posibilidad de error o viendo la funcionalidad manualmente. La coleccion de datos tiene una cabecera baja, menos del 2%. La coleccion de datos es también escalable, lo cual es muy importante en el crecimiento del sistema. Como el numero de usuarios aumenta, las aplicaciones son sumadas o la infraestructura global crece, dandole continuidad a la colección de datos sin interrupción, omision, intervención manual o incremento en la cabecera.

La coleccion de datos del software de Patrol esta sustentada por una solución de la administración funcional de Patrol. La tasa de captura de datos de Patrol es cerca del 100%.

Patrón para servidores Microsoft Windows esta diseñado para monitorear y administrar dentro del medio de Servidores Microsoft (Microsoft Windows NT, servidores Microsoft Windows 2000,

Microsoft Windows 2000 Advanced Server y Microsoft Windows 2000 Datacenter Server). Este producto ofrece en una sola compra la aplicación de administrar los clientes de servidores NT y Windows 2000. Este único producto puede trabajar con ambos servidores NT y 2000. Este incluye monitoreo para OS (Operation Systems) por si mismo, monitoreo de campo, monitoreo IIS, notificacion de alerta y es extensible a traves de Patrol PerfMon Wizard. Esencialmente, este producto permite al cliente detectar condiciones de alarma, notifica al personal de soporte acerca de las condiciones de alarma y algunos casos corrigen los problemas que ocurran dentro de sus ambientes en aplicaciones de grupo o distribucion.

IP Optimizer CycloneFrame

IP Optimizer es una herramienta avanzada de resolución de problemas, basada en el protocolo IP. Sus funciones principales se basan en monitorear, mantener y resolver los problemas de las redes de datos con máxima eficacia y productividad. Es un sistema con análisis en tiempo real del flujo de tráfico y las conversaciones, no se limita a decodificar los mensajes. Monitorea la red y avisa de los problemas potenciales antes de que ocurran. Localiza rápidamente las áreas problemáticas e indica posibles soluciones.

Sus funciones comprenden:

- Permite acceder tanto a los servicios IP como a protocolos más antiguos
- Soporta todas las tecnologías de acceso utilizadas por los operadores de redes de datos.
  Frame Relay y servicios de datos con lineas alquiladas
  HDLC, Cisco, PPP y X.25
- Interfaces estándar.
  T1, 2M, DDS, V.35, RS232, RS449, X.21 y RS530
- Interfaz gráfica de usuario clara e intuitiva
- Motores de análisis expertos centrados en la WAN
- Ofrece flexibilidad remota
- Ejecuta las aplicaciones en las instalaciones del cliente o en la oficina central
- Permite el acceso remoto mediante comunicación telefónica estándar, con protocolo IP

La interfaz grafica de usuario, clara e intuitiva, automatiza las fases de configuración, procesamiento y decodificacion, ofreciendo al usuario análisis avanzados con resultados gráficos y textuales, e información completa sobre el estado de la red.

El CycloneFrame se basa en un motor de análisis experto que analiza y detecta automáticamente los problemas de la red en tiempo real. Cuando ocurre un evento, el CycloneFrame lo registra y le añade la referencia temporal correspondiente.

Identifica la fuente de utilización y los problemas de conectividad, y determina la extensión de los errores. También relaciona los eventos asociados, mostrándolos en gráficos fáciles de entender que clarifican la raíz del problema, y recomienda las soluciones más aconsejables, lo que reduce el tiempo necesario para la resolución.

Flexibilidad local y remota.

El CycloneFrame IP Optimizer da a sus ingenieros la libertad de operar de muchas maneras diferentes para satisfacer sus necesidades, debido a que puede conectarse a cualquier punto de la red mediante el hardware direccionable IP, para accesar a los resultados. Para las pruebas remotas, se puede conectar mediante una tarjeta NIC 10/100 BaseT, a través de una LAN compartida, sobre una red IP, o incluso mediante una conexión telefónica. También puede conectarse directamente a una computadora portatil.

Máxima compatibilidad.

Dado que el tráfico IP que atraviesa la red basada en tramas utiliza un amplio conjunto de protocolos estándar, el CycloneFrame soporta los protocolos más modernos, pero también los más antiguos. Entre las aplicaciones soportadas se cuentan las basadas en WWW/HTTP, correo electrónico, VoIP (voz sobre IP) y VPN (red privada virtual). El CycloneFrame también soporta las tecnologías relacionadas con los accesos, como Frame Relay. El CycloneFrame puede acceder a las interfaces estándar, como T1, 2M, DDS, V.35, X.21, RS232, RS449 y RS530.

El CycloneFrame permite comprobar asimismo las redes punto a punto con líneas T1/E1 alquiladas o privadas y circuitos DDS/56k en la capa física. Generalmente estos circuitos utilizan en la capa 2 los protocolos PPP, Cisco HDLC o HDLC genérico, en vez de Frame Relay.

4.2.2 Sofware Libre

Existen en el mercado varias asociaciones o grupos independientes que se dedican al desarrollo de software que ayuda al monitoreo de las redes, donde su principal característica es ofrecer al mercado la disponibilidad de sus productos sin costo alguno.

Trabajar con alguno de estos softwares se recomienda cuando la Empresa no tiene los recursos suficientes para invertir en la compra de software más especializado. Algunos de los productos son lo suficientemente confiables para implementarse en las redes, aunque la desventaja principal es la dependencia al desarrollador que libera los productos sin el control de seguridad y funcionalidad necesario.

A continuación se mencionan algunos de los softwares comerciales libres que pueden utilizarse:

ACID (Analysis Console for Intrusion Databases).

Herramienta de análisis utilizada para procesar las bases de datos de los registros generados por los firewall y las herramientas de monitoreo de la red. Sus funciones incluyen:

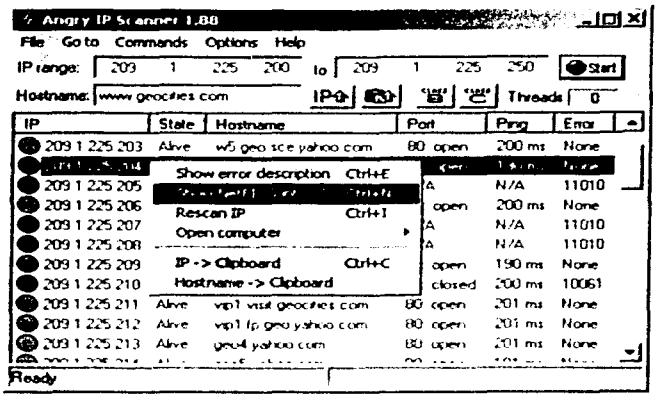
- Creación de filtros y búsquedas para localizar información sobre el Sistema de Monitoreo, por ejemplo, a que hora se detectó la alarma, quien esta conectado, así como la fuente de origen del problema, por ejemplo: direcciones de fuente/destino, puertos, banderas encendidas.
- Decodificador. Herramienta gráfica que mostrará información sobre las alarmas registradas
- Administrador de Alertas. Su función es la construcción de un grupo lógico de alertas, cuya finalidad es la de borrar las alarmas falsas o verdaderas mediante el envío de correos electrónicos a los responsables de la red o exportando la alerta a una base de datos de alarmas.
- Grafica y genera estadísticas basadas en tiempo, protocolos, direcciones IP, puertos TCP/UDP o por clasificación de alertas.
- ACID tiene la capacidad de analizar una amplia variedad de eventos que son post-procesados en su base de datos.

Angry IP Scanner

Angry IP Scanner es una herramienta muy rápida para detectar las direcciones IP sobre Windows. Angry IP Scanner puede detectar direcciones IP desde 1.1.1.1 a 255.255.255.255 Su instalación es muy facil y el archivo ocupa un tamaño muy pequeño comparado con otros exploradores IP.

Angry IP envia simplemente pings a cada dirección para comprobar si están activas, entonces al resolver el nombre del servidor intenta conectarse al hostname.

También provee información del NetBIOS tales como el nombre de la computadora, el nombre del grupo de trabajo, usuarios conectados y la MAC adress, los cuales son guardados en formatos txt para mayor facilidad de manejo.



Pantalla principal de Angry IP scanner

BIG BROTHER

Big Brother es el primer software de monitoreo creado en 1996, capaz de monitorear redes a través de accesos vía WEB.

Big Brother monitorea los sistemas y la disponibilidad de los servicios entregados a través de la red. El status actual de la red es desplegado en una página de WEB con tiempos muy cercanos al real, codificados en color. Cuando un problema se detecta, se envía inmediatamente una notificación por correo electrónico o por radio localizador.

El archivo fuente del código está diseñado para plataformas Unix y Linux y se precompila para Windows NT y 2000, aunque también esta disponible para redes Mac, OS/9, AS/400 y VM/ESA.

No report

- No existen reportes del cliente en los últimos 30 min. La conexión pudo haberse interrumpido

Attention

- El sistema de reporteo rebaso el umbral y puede interrumpirse.

■ **OK**
Todo esta bien.

Unavailable
Las pruebas han sido apagadas o no se están aplicando. Un ejemplo puede ser la conectividad o desconectividad de los accesos telefónicos de las redes (dialup lines)

Disabled
● Notificación que indica la incapacidad del sistema. Por ejemplo cuando se esta utilizando para dar mantenimiento.

✓✓ **Acked**
Un evento actual ha sido reconocido por uno o varios destinatarios.

Todas las conexiones son revisadas cada 5 minutos.

La mayoría de los resultados críticos, son notificados al administrador. Estos incluyen: la pérdida de conectividad de la red, la perdida de acceso del HTTP y la saturación del disco duro al 95%, debido a que estos pueden dar lugar a una caída del sistema.

Entre los parámetros que examina y que reporta, se encuentran:

- Envió de pings periódicos
- Revisión del NNTP
- Comprobación de CPU
- Capacidad del disco duro
- Verifica el estado del servidor DNS
- Verificación de los protocolos FTP, http, SMTP
- Conectividad del servidor

Dynu DNS Query

Dynu DNS Query, es una herramienta para la búsqueda de parámetros en el servidor de Nombre de Dominio (DNS)

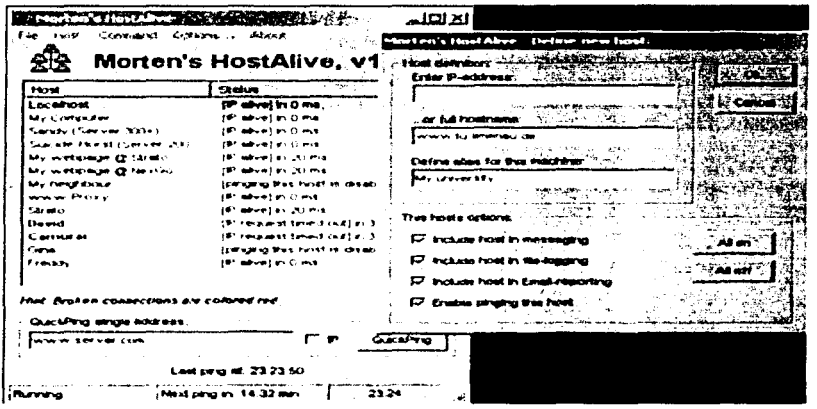
El nombre del servidor puede ser utilizado como entrada para la búsqueda, el nombre del servidor de la máquina por omisión será utilizada automáticamente. Una bitácora de actividades muestra claramente el estado de la búsqueda. Los resultados incluyen información detallada sobre parámetros tales como: TTL (Time to Live), señación, refrescamiento, reintento y expiración.

A continuación se enlistan los registros que Dynu DNS query puede detectar:

- Host Address
- Name Servers
- Mail Exchange
- Mail Destination
- Mail Forwarder
- Start of Authority
- Canonical Name
- Text Entries
- Host Information
- Domain Pointer
- MailBox
- MailGroup
- Mail Rename

Morten's HostAlive

Morten's HostAlive es una herramienta de multi ping que sirve para comprobar en línea el estado de la computadora en una red TCP/IP. El sistema es bastante fácil, sólo requiere que se agregue en una lista los host que quiere revisar (soporta direcciones IP y los nombres de dominio); el intervalo de tiempo para cada envio de ping y Morten HostAlive reportará el estatus de la máquina.



Pantalla principal de Morten HostAlive

INetTools

INetTools es una colección de herramientas de prueba para redes IP e Internet.
La colección de herramientas InetTools incluye la consulta de DNS, localización de nombres, ping scan, localización de puertos y la detección de rendimiento de la red y de rutas remotas. La interfaz del usuario le permite accesar a la información, sin la necesidad de recordar las sintaxis de los parámetros de linea.

Los parámetros que puede analizar son:

- Ping.- Envía un número de paquetes de ping en determinado intervalo de tiempo y lista los registros que tardan en responder cada paquete.
- DNS Lookup .- Proporciona información detallada en el host de Internet. Es una herramienta para la búsqueda del "Domain Name Servers".
- Name Lookup .- Utiliza la DNS para cambiar de nombres a direcciones y de direcciones a nombres.
- Finger.- Utiliza el protocolo Finger para obtener información sobre el usuario que está trabajando en la computadora o en Internet
- Whois .- Utiliza el protocolo Whois para obtener información sobre su propio Dominio.
- Throughput .- Pruebas sobre la disponibilidad de los recursos en Internet (FTP o http) para calcular los tiempos, tamaños y velocidad en que se instala un archivo.
- Name Scan .- Toma el inicio y el final de la dirección IP para localizar los nombres de todos los dispositivos asociados con esa dirección.
- Localización de puertos - Localiza los puertos del equipo para servicios de FTP, http y Telnet.
- Ping Scan.- Con el inicio y el termino de la dirección IP, se envían pings a cada dirección para determinar cual es la que está actualmente en uso
- Service Scan.- Proporcionando el inicio y el termino de la direccion IP, Service Scan verifica cada direccion IP para determinado servicio, por ejemplo, FTP,http,etc.

Ping Plotter

Ping Plotter es un programa de ruteo para Windows 95/98/NT. Proporciona los elementos para trazar rutas mas rapidas y mejores, ademas de poseer graficadores, estadisticas, monitoreo a largo plazo y alarmas.
Ping Plotter fue escrito para ayuda a solucionar las conexiones de Internet, pero no es ningún programa de ruta de rastreo regular.

4.2.3) Herramientas de monitoreo

Estas herramientas se encuentran integradas en algunos sistemas operativos.

NETSTAT

El comando NETSTAT esta presente en la mayoría de los sistemas operativos y es un comando que se utiliza para presentar el estado de la red. Proporciona una variedad de información y es comúnmente usado para presentar estadísticas detalladas acerca de cada interfaz de red, sockets y tablas de ruteo.

TCPDUMP

Es un programa para sistemas UNIX que se usa para monitorear el tráfico de paquetes TCP/IP sobre una red Ethernet. Los problemas causados por una mala configuración de TCP/IP son mucho más comunes que los ocasionados por malas implementaciones de TCP/IP. En ocasiones es necesario analizar la interacción de protocolo entre dos sistemas y en el peor de los casos se necesitará analizar los paquetes bit por bit.

4.3 Monitoreo de Seguridad

Introducción

En estas páginas nos centraremos en la seguridad en la comunicación a través de redes, especialmente Internet, consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información, más que en la seguridad en las computadoras, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, mas que físicos.

La evolución de las nuevas tecnologías, en especial el tremendo auge de las tecnologías Internet/Intranet, ha provocado la aparición de nuevas necesidades y la posibilidad de adquirir ventajas competitivas. Además hay que aclarar que lo que inicialmente partió como una opción de negocio se esta transformando en una elección obligada si se desea mantener la posición en el mercado frente a los competidores.

Los beneficios atribuibles a las nuevas tecnologías son muchos, pero también los riesgos: la pérdida de imagen (a menudo mas crítica que la propia pérdida de datos), la pérdida de información, la suplantación de usuarios, el espionaje de información sensible o incluso el cumplimiento de la normativa vigente.

A pesar de lo cambiante del entorno, los requisitos de seguridad siguen siendo los mismos: Autenticación, confidencialidad, control de acceso, integridad y no repudio; aunque los objetivos y la implementación de los mismos evoluciona a velocidad vertiginosa.

La Problemática de Seguridad

A lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas y organismos han sido una constante recurrente; se pueden diferenciar en tres grandes grupos:

- Los problemas estructurales

Habitualmente la estructura de la organización no se hace pensando en la seguridad por lo que no hay una definición formal de las funciones ni responsabilidades relativas a seguridad.

No suelen existir canales de comunicacion adecuados para tratar incidentes de seguridad, predominando los canales de tipo informal y el de boca a boca.

Exceptuando determinados ambientes como la banca o la defensa, no suelen existir recursos especificos dedicados a seguridad, y cuando existen suelen dedicarse a la seguridad física (puertas, alarmas, dispositivos anti-incendios, etc.) por ser más facilmente justificable su adquisición.

- Problemas en el planteamiento

Los planteamientos de seguridad suelen adolecer de falta de coherencia ya que no suelen ser ni suelen estar adaptados a las necesidades de la empresa.

Habitualmente las directrices no son homogéneas en toda la organización.

Como consecuencia de la falta de definición de funciones, nadie quiere responsabilizarse de los riesgos asumidos en la organización y nadie quiere adoptar medidas que puedan dificultar el proceso de negocio.

No se definen normas ni procedimientos salvo cuando su ausencia puede afectar al propio negocio (por ejemplo la existencia de copias de seguridad) o tras un incidente grave de seguridad

Al no existir beneficios inmediatos, resulta difícil justificar gastos y recursos.

- El problema tecnológico

A pesar de la opinión generalizada, la tecnología no es la panacea; las herramientas son un soporte, pero si no hay una base con ideas sólidas no solucionan los problemas.

Además, las herramientas existentes, de por sí, no cubren todas las necesidades.

La sensación de falsa seguridad provocada por la excesiva confianza en las soluciones tecnológicas induce a bajar la guardia.

Resumiendo; la situación real suele ser que en las empresas y organismos, el negocio y la imagen se anteponen a la seguridad. La organización crece e implementa soluciones de seguridad de acuerdo a necesidades puntuales, no hay definida una estrategia, ni normas ni procedimientos, es decir, lo habitual es que no se contemple expresamente la seguridad.

El problema principal que se desprende de todo lo anterior es que normalmente no se conoce el riesgo que se está asumiendo.

Planificando la Seguridad

Una vez identificados los problemas generales llega la pregunta que supone el principal escollo para desarrollar un plan que corrija la situación: ¿Cómo se debe abordar la seguridad en la organización?

El Plan de Seguridad debe ser un proyecto que desarrolle los objetivos de seguridad a largo plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión.

La forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una política de seguridad que defina el QUÉ se quiere hacer en materia de seguridad en la organización para a partir de ella decidir mediante un adecuado plan de implementación el CÓMO se alcanzarán en la práctica los objetivos fijados.

La Política de Seguridad englobará pues los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de un análisis de riesgos, la definición de normativa y procedimientos, la definición de planes de contingencia ante desastres y la definición del plan de auditoría.

A partir de la Política de Seguridad se podrá definir el Plan de Implementación, que es muy dependiente de las decisiones tomadas en ella, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad. Es necesario que la política sea aprobada para que este respaldada por la autoridad necesaria que asegure su cumplimiento y la asignación de recursos.

Amenazas en la Seguridad

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). 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.

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 una computadora. 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 desvelar 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 transfendos 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 falsos 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 trafico, una técnica mas 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 periodos 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 que se verán más adelante.

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 millon de dólares en la cuenta A" podría ser modificado para decir "Ingresa un millón de dólares 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. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

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 falso al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos metodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

- Autentificación: 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 comunicacion, 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 mediante técnicas básicas.

- 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 resolucion 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 informatico esten disponibles a las entidades autorizadas cuando los necesiten.

Mecanismos de Seguridad

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.

- Control de acceso: esfuerzo para que solo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

- Tráfico de relleno: consiste en enviar tráfico falso 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 solo 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.

Criptología

Se entiende por criptología el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.

La Criptografía es la parte de la Criptología que estudia como cifrar efectivamente los mensajes.

En algunos países está directamente prohibido el uso de mensajes cifrados (como Francia o China, por ejemplo), en otros como Estados Unidos está fuertemente controlado, impidiéndose la exportación de programas cifradores al considerarse por el Acta de Control de Exportación de

Armas (Arms Export Control Act) como incluida en su lista, junto a misiles, bombas y armamento diverso.

Hay muchos países que, aunque en su territorio nacional permiten el uso de la Criptología, desean que estos programas incluyan una puerta trasera (backdoor) o procedimiento parecido para poder intervenir el mensaje cuando así lo consideren oportuno: Es el caso del famoso chip de depósito de claves o Chip Clipper, para cifrar conversaciones telefónicas (los dos teléfonos participantes en una conversación deben tenerlo).

Todo esto lleva directamente al enfrentamiento de la privacidad en las comunicaciones-control gubernamental. Lo cual desemboca en la posible afectación de derechos fundamentales de las personas, como es el derecho a la libertad de expresión, que difícilmente se puede conseguir si cuando nos comunicamos con alguien no sabemos quien o quienes pueden realmente leer el mensaje y el derecho a la privacidad. Problema que se agrava en Internet, ya que los mensajes se pueden quedar en el ciberespacio por tiempo indefinido, sin tener nosotros siquiera conciencia de ello o de donde estará efectivamente copiada o almacenada nuestra comunicación.

La cuestión es conseguir que aunque los mensajes puedan ser interceptados, resulten totalmente ininteligibles. Y esto se consigue con la Criptología.

No es un problema trivial: es de vital importancia para que se desarrolle el comercio seguro en Internet, para los grupos defensores de los Derechos Humanos o para las comunicaciones entre abogados y sus clientes, por indicar algunos de los cientos de ejemplos posibles.

Este sistema de clave pública y clave privada se conoce como sistema asimetrico.

La tendencia de los sistemas de clave simetrica, actualmente, es a utilizarlos poco o simplemente para cuestiones que no necesiten un alto grado de protección.

Los sistemas de clave asimétrica son los que se están imponiendo, ya que ofrecen un mayor grado de seguridad. Sobre todo porque no hace falta que la clave sea conocida nada más que por una persona. Ya se sabe que cuando un secreto se comparte, hay bastantes posibilidades para que deje de serlo.

Entre los programas cifradores de esta segunda clase, el que se está configurando como un standard (por lo menos en cuanto a los usuarios corrientes) y goza de mayor popularidad es el PGP o Pretty Good Privacy (Privacidad Bastante Buena) de Phil Zimmermann, basado en un sistema de doble clave (una pública y otra privada). Existe tanto en versiones gratuitas como comerciales.

Gestión de Claves

Abarca la generación, distribución, almacenamiento, tiempo de vida, destrucción y aplicación de las claves de acuerdo con una política de seguridad.

Generación de claves

La seguridad de un algoritmo descansa en la clave. Un criptosistema que haga uso de claves criptográficamente débiles será el mismo débil. Algunos aspectos a considerar que se presentan a la hora de la elección de las claves son:

- Espacio de claves reducido
  Cuando existen restricciones en el número de bits de la clave, o bien en la clase de bytes permitidos (caracteres ASCII, caracteres alfanuméricos, imprimibles, etc.), los ataques de fuerza bruta con hardware especializado o proceso en paralelo pueden desbaratar en un tiempo razonable estos sistemas.

- Elección pobre de la clave
  Cuando los usuarios eligen sus claves, la elección suele ser muy pobre en general (por ejemplo, el propio nombre o el de la mujer), haciéndolas muy débiles para un ataque de fuerza bruta que primero pruebe las claves más obvias (ataque de diccionario).

Claves aleatorias

Claves buenas son las cadenas de bits aleatorios generadas por medio de algún proceso automático (como una fuente aleatoria fiable o un generador pseudo-aleatorio criptográficamente seguro), de forma que si la clave consta de 64 bits, las 264 claves posibles sean igualmente probables. En el caso de los criptosistemas de clave pública, el proceso se complica, ya que a menudo las claves deben verificar ciertas propiedades matemáticas (ser primos dos veces seguros, residuos cuadráticos, etc.).

Frases de paso

Esta solución al problema de la generación de contraseñas seguras (y fáciles de recordar) por parte del usuario consiste en utilizar una frase suficientemente larga que posteriormente es convertida en una clave aleatoria por medio de un algoritmo (key-crunching).

Distribución de claves

Sin duda alguna, el problema central de todo sistema de gestión de claves lo constituyen los procedimientos de distribución de éstas. Esta distribución debe efectuarse previamente a la comunicación. Los requisitos específicos en cuanto a seguridad de esta distribución dependerán de para que y como van a ser utilizadas las claves. Así pues, será necesario garantizar la identidad de su origen, su integridad y, en el caso de claves secretas, su confidencialidad.

Las consideraciones más importantes para un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger. Esta distribución es automática y la transferencia suele iniciarse con la petición de clave por parte de una entidad a un Centro de Distribución de Claves

(intercambio centralizado) o a la otra entidad involucrada en la comunicación (intercambio directo). La alternativa es una distribución manual (mediante el empleo de correos seguros, por ejemplo), independiente del canal de comunicación. Esta última alternativa implica un alto costo económico y un tiempo relativamente largo para llevarse a cabo, lo que la hace descartable en la mayoría de las situaciones. La distribución segura de claves sobre canal inseguro requiere protección criptográfica y, por tanto, la presencia de otras claves, conformando una jerarquía de claves. En cierto punto se requerirá protección no criptográfica de algunas claves (llamadas maestras), usadas para intercambiar con los usuarios de forma segura las claves que usarán en su(s) futura(s) comunicación(es). Entre las técnicas y ejemplos no criptográficos se puede citar seguridad física y confianza.

La distribucion de claves se lleva siempre a cabo mediante protocolos, es decir, secuencias de pasos de comunicacion (transferencia de mensajes) y pasos de computación. Muchas de las propiedades de estos protocolos dependen de la estructura de los mensajes intercambiados y no de los algoritmos criptográficos subyacentes. Por ello, las debilidades de estos protocolos provienen normalmente de errores cometidos en los niveles más altos del diseño.

Las claves criptográficas temporales usadas durante la comunicación, llamadas claves de sesión, deben ser generadas de forma aleatoria. Para protegerlas será necesaria seguridad física o cifrado mediante claves maestras, mientras que para evitar que sean modificadas deberá utilizarse seguridad física o autenticacion. La autenticacion hace uso de parámetros como time-stamps y contadores para protegerse tambien contra la reactuación con antiguas claves.

Almacenamiento de claves

En sistemas con un solo usuario, la solución más sencilla pasa por ser su retención en la memoria del usuario. Una solución mas sofisticada y que desde luego funcionará mejor para claves largas, consiste en almacenarlas en una tarjeta de banda magnetica, en una llave de plástico con un chip ROM (ROM key) o en una tarjeta inteligente, de manera que el usuario no tenga más que insertar el dispositivo empleado en alguna ranura a tal efecto para introducir su clave.

Otra manera de almacenar claves difíciles de recordar es en forma encriptada mediante una clave facil de recordar, como por ejemplo almacenar en disco la clave privada RSA cifrada mediante una clave DES.

Tiempo de vida de claves

Una clave nunca debería usarse por tiempo indefinido. Debe tener una fecha de caducidad, por las siguientes razones:

- Cuanto más tiempo se usa una clave, aumenta la probabilidad de que se comprometa (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).

- Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, ya que toda la información protegida con esa clave queda al descubierto.

- Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar desbaratarla.

En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

Para protocolos orientados a conexión, una elección obvia es usar la misma clave de sesión durante la duración de la comunicación, siendo descartada al finalizar la comunicación y nunca reutilizada. Si la conexión lógica posee una vida muy larga, sería prudente en este caso cambiar la clave de sesión periódicamente, por ejemplo cada vez que el número de secuencia de la PDU completa un ciclo.

Para protocolos no orientados a conexión, no existe un inicio o fin de sesión explícitos. Por lo tanto, no resulta tan obvio con qué frecuencia debería cambiarse la clave. Con el fin de no recargar la información de control ni retrasar la transacción, una estrategia válida sería usar una clave de sesión durante un cierto período o para un cierto número de transacciones.

Las claves maestras no necesitan ser reemplazadas tan frecuentemente, ya que se usan ocasionalmente para el intercambio de claves. En cualquier caso, no hay que olvidar que si una clave maestra se compromete, la pérdida potencial es enorme, de hecho, todas las comunicaciones cifradas con claves intercambiadas con esa clave maestra.

En el caso del cifrado de grandes archivos de datos, una solución económica y segura, mejor que andar descifrando y volviendo a cifrar los archivos con una nueva clave todos los días, sería cifrar cada archivo con una única clave y después cifrar todas las claves con una clave maestra, que deberá ser almacenada en un lugar de alta seguridad, ya que su pérdida o compromiso echaría a perder la confidencialidad de todos los archivos.

Destrucción de claves

Las claves caducadas deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de un adversario, puesto que con ellas podría leer los mensajes antiguos. En el caso de haber sido escritas en papel, este deberá ser debidamente destruido; si habían sido grabadas en una EEPROM, deberá sobrescribirse múltiples veces, y si se encontraba en EPROM, PROM o tarjeta de banda magnética, deberán ser hechas añicos (muy pequeñitos, a poder ser). En función del dispositivo empleado, deberá buscarse la forma de que se vuelvan irrecuperables.

4.3.1 Software de Seguridad

FIREWALL

Una firewall es una barrera que controla el flujo del tráfico entre los host, los sistemas de redes, y los dominios. Existen diferentes clases, las más débiles; y las más seguras, que deberían bloquear el traspaso de cualquier tipo de datos.

Un Firewall es un tipo de tecnología que ayuda a prevenir el acceso de intrusos a tu computadora, ya sea por medio de Internet o por medio de una Red Interna; además de controlar la entrada o salida de datos, no autorizada, a un sistema.

El concepto de firewall proviene de la mecánica automotriz, donde se le considera una lámina protectora / separadora entre el chasis de un vehículo y las partes combustibles del motor, que protege a sus pasajeros en caso de incendio. Análogamente, un firewall, en un sentido más informático, es un sistema capaz de separar el interior de nuestra red, o sea, del posible incendio de crackers que se produciría en ese gran motor que es Internet.

En otras palabras, un firewall garantiza que si la red tiene algún tipo de conexión hacia el mundo exterior, o hacia otras redes, ésta sea segura, evitando violaciones, y permitiendo pasar sólo los paquetes de red autorizados, por lo que se deben configurar los firewalls para lograr que sean transparente a los usuarios normales de la red, y totalmente sólido para los "otros usuarios".

En muchos casos, la posibilidad de destrucción de la información existente en la red, por medio de los llamados "hackers" (en realidad, el término correcto es el de crackers), lleva a implementar la necesidad de, en caso de conectarse con redes externas, loguearse primero en un computadora firewall, y luego salir hacia el exterior.

Esta política no es la mas acertada, ya que el sólo hecho de saber que hay un firewall, lleva a usuarios mas conocedores en el mundo de las redes a intentar crackearlos, muchas veces con éxito por tener más datos de la red que los crackers externos.

En el año 1997, el 85% de los problemas de seguridad fueron ocasionados por usuarios internos, desde la propia red en la que se estaba trabajando, que intentaban, como meta personal, lograr destruir la seguridad interna.

Sin duda el mejor firewall es el que no genera una huella visible en una red. Es el que posee un sistema operativo que es totalmente desconocido, o que no posee un sistema operativo en el concepto completo que todos poseemos del mismo. Hoy en día, existen productos que permiten, a través de algoritmos muy avanzados, generar redes privadas virtuales en Internet, a través de la desaparición de las máquinas que se están conectando, ya que el nuevo protocolo no necesita de dirección IP para lograr el éxito de la comunicación. El mismo se basa en el concepto de la creación de un "túnel" dentro de Internet.

La ventaja de estos sistemas, es que el cracker no encuentra que es lo que debe crackear, ya que estos sistemas no permiten el sniff.

La desventaja es que sólo se puede generar la comunicación si de los dos lados de la red existe un sistema con estas características. Sin embargo, se puede armar un sistema bastante seguro utilizando un Sistema Operativo robusto, el software adecuado, y las configuraciones necesarias para tales fines.

Sistemas de seguridad Firewalls

Existen algunos tipos de paquetes que se desea se ingresen a la red, y algunos que se desean, como un cable a tierra, que sean automáticamente descartados. Este proceso se llama filtrado de paquetes, y su existencia valida la de los llamados "Filtering Firewalls" ó "IP Packet Filtering Firewalls", sistemas que se ocupan, tal como lo hace un filtro de café, de permitir pasar la información de los paquetes autorizados, y de filtrar la parte no deseada de los paquetes no autorizados.

Para realizar este filtrado, el sistema observa la fuente, el destino, el puerto, el tipo de paquete, y revisa algo de su contenido, en busca de elementos nocivos para la red; si se descarta todo lo que nos resulta nocivo, lo hace también con cualquier tipo de log que pueda demostrar la existencia de estos elementos, ya que el sólo hecho de poseer la capacidad de escribir en disco, a veces es utilizada por crackers para incluir, en el mismo log, un caballo de troya (programas destructivos que están a la espera de la ejecución de alguna acción sobre ellos, tales como la lectura) que afectarían el funcionamiento del firewall. Esto incluye la posibilidad de incluir algún tipo de antivirus, o algun otro tipo de sistemas de protección para los paquetes que sí se quieren que ingresen.

Pero existe ya un sistema de vigilancia, que verifica todos los paquetes de red salientes, evitando dejar brechas abiertas, y separando la "pulcritud de la red", del desorden externo, además verifica cada uno de los paquetes entrantes, luego de haber sido filtrados por un firewall, este sistema es Proxy server, también conocido como aplicación Gateway, o Forwarder. Este no es más que un sistema intermedio, que se ocupa de habilitar un movimiento indirecto de paquetes de red, desde la maquina interna hasta el firewall, y de allí a la red externa. El se ocupa de, ante un pedido de información interna, loguearse al firewall, obtener la misma, y proporcionarla a los usuarios. También, algunos proxies, contienen loggeo (observar la doble g) interno, y soporte para autenticacion de usuarios. Dado que un proxy debe entender el protocolo de la aplicacion utilizada, tambien puede implementar seguridad especifica para ese protocolo (por ejemplo, un proxy de http, puede permitir las conexiones entrantes, y no las salientes).

El objetivo de los cyberataques de los Hackers no es precisamente atacar a las organizaciones de seguridad; lo que ellos siempre intentan es buscar numeros de cuentas bancarias, claves, etc. Por otro lado, el surgimiento de las conexiones permanentes hacia la Red, como por ejemplo, el cable modem entre otros, se está volviendo cada vez más popular, sobre todo entre los usuarios que necesitan estar la mayoría del tiempo online, para poder realizar su trabajo. De esta manera, el peligro de las invasiones a la red crecen día a día, y los hackers tienen más posibilidades de realizar mas facilmente su tarea.

Un firewall puede impedir que un usuario no autorizado acceda a la PC, independientemente de donde provenga el, es decir, puede provenir de la Web o de la red local. Bloquea algunos programas troyanos y otras aplicaciones que quieren dañar el sistema.

Mientras se esta conectado a la Web, constantemente se está enviando y recibiendo información en pequeñas unidades llamadas paquetes. Un paquete contiene la dirección de

quien envía el mensaje, y del receptor, junto con una porción de información, una petición, y un comando. Pero al igual que con los mail, no siempre se recibe en la computadora todos los paquetes de información que se desea, ya que a veces, algunos son completamente innecesarios.

Un firewall examina cada paquete enviado desde o hacia la computadora, para analizar si cumple con una serie de criterios; así, luego puede decidir si permite o no el paso del paquete de información.

El criterio que este tipo de aplicaciones utiliza para dejar o no pasar el paquete depende del tipo de firewall que se utilice. El tipo más común que se encuentra para las computadoras personales y para las medianas empresas se denomina Aplicación Gateway Firewall (es decir, Sistema de Protección de Entrada para las Aplicaciones).

Una aplicación gateway, comúnmente llamada proxy, es una especie de "Oficial de aduanas" para los datos: cualquier cosa que se envíe o reciba primero pasa por la firewall, que filtra los paquetes en base a las direcciones IP y al contenido, así como también, en base a las funciones específicas de cada aplicación. Por ejemplo, si se está ejecutando un programa de FTP, el proxy podría permitir la carga de archivos mientras bloquea otras funciones, tales como la visualización o el borrado de los archivos. También se puede configurar al firewall para que ignore todo el tráfico de los servicios de FTP, pero para que autorice la circulación de todos los paquetes generados durante la navegación.

Otros tipos de firewall incluyen filtros que examinan la dirección IP de cada paquete para aprobarla o no; otros que controlan los niveles de los circuitos de la información, los cuales permiten la comunicación sólo entre las computadoras admitidas y los proveedores de servicios de Internet; y por último, una nueva clase de barrera conocida como firewall de inspección de estados, que controla las configuraciones de cada paquete aprobado y luego pasa o bloquea el tráfico basado en dichas características.

Estos tres tipos de firewall se encuentran más comúnmente en los sistemas empresariales en donde la seguridad y protección de la información es una condición indispensable para el trabajo, ya que además, son aplicaciones que requieren un mantenimiento importante, por lo tanto no son útiles en las pequeñas empresas o en los sistemas hogareños.

NORTON PERSONAL FIREWALL 2002

En su versión 2002, ofrece una respuesta plausible a estas necesidades, garantizando la inviolabilidad de accesos hacia adentro de nuestra red local o de nuestro equipo, mediante el establecimiento de simples reglas de seguridad, tanto para programas que deben de acceder a Internet (obligando a las conexiones a abrir determinados puertos de comunicación que pueden resultar no seguros), como controlando a que zonas se puede acceder libremente.

MCAFEE FIREWALL

El proceso de configuración es rápido y sencillo, sin que ello afecte negativamente a la seguridad. McAfee Firewall se integra de forma transparente y sin problemas con el entorno de escritorio existente al mismo tiempo que controla las amenazas a la seguridad del sistema.

El software McAfee Firewall filtra todas las aplicaciones, los servicios de sistema y los protocolos, incluida la compartición de impresora y de archivos (NetBIOS); protocolos IP (TCP/IP, UDP/IP); protocolos basados en servicios (FTP, Telnet); ARP/RARP y DHCP. Además, bloquea IPX y NetBEUI en cada dispositivo. Las normas del software McAfee Firewall están creadas basándose en aplicaciones. Cuando utilice un programa nuevo para conectarse a Internet, el software McAfee Firewall le preguntará si confía en la aplicación. Si confía en el programa, le permitirá comunicarse con Internet. En caso contrario, se bloquearán todas las comunicaciones con dicho programa. Este sistema asegura que el usuario está informado de las aplicaciones que intentan acceder a Internet y le otorga la facultad de poder conceder permiso o denegarlo.

Puede personalizar estas normas para que se adapten a sus hábitos de navegación.

FireWall OfiServer-FW

Es un sistema integral de seguridad que protege la presencia de su empresa en Internet y el cual ha sido diseñado para ser fácil de usar, flexible y por supuesto muy seguro.

El OfiServer no sólo ha sido diseñado para integrarse fácilmente en una red existente, sino que además no requiere de un administrador de red experto para operarlo. Al momento que se conecta y enciende, por medio del módulo de administración se configura la red. Una vez conectado, el mismo módulo de administración le facilita dar de alta usuarios y grupos, activar servicios o implementar políticas de seguridad. Toda la administración se realiza a través de un explorador Web.

El OfiServer incluye un módulo de administración vía Web para configurar la red interna para usar DHCP, DNS, NAT y Servicios Web.

Nos proporciona un proceso integrado de monitoreo y de reportes que detallan cuando los servicios de seguridad son utilizados y con esto conocer los intentos de intrusión para poder tomar medidas sobre quienes los provocan. Se integra con el Servidor Proxy, con el FireWall y con el servicio de "Web Caching" para evitar que el contenido no autorizado de Internet sea accesado por los empleados. Permite monitorear, obtener reportes y controlar el tráfico de su red interna para ayudar a su empresa a conservar el preciado ancho de banda, incrementar la productividad de los empleados y reforzar las políticas de acceso a Internet de su empresa.

IBM ENETWORK FIREWALL V3.3 PARA AIX Y NT

Los productos de IBM ENetwork (TM) Firewall protegen sus redes de intervenciones externas gracias a:

- La autorización del tráfico únicamente a través del Firewall que se haya autorizado explícitamente.

- El "fortalecimiento" del sistema en el que se ejecuta el Firewall, que reduce la posibilidad de que algún "hacker" pueda acceder al cortafuego o atravesarlo.

- La ocultación de direcciones IP y de la configuración de la red interna a la red de baja fiabilidad.

- La posibilidad de archivar cronológicamente todo el tráfico a través del cortafuego y utilizarlo para generar informes sobre la actividad del usuario.

FIRE WALL-1 CHECK POINT (Tecnologia Tateful Inspection)

Desarrollado por Check Point Software Technologies (http://www.checkpoint.com), está basado en la arquitectura de Stateful Inspection, la nueva generación de tecnología de firewall inventada por Check Point. La tecnología de inspección de estado ofrece funcionalidad completa de firewall y asegura el nivel más alto de seguridad para la red.

Inspection Module de FireWall-1 analiza todos los niveles de comunicaciones y el estado de la aplicación. El Inspection Module entiende y puede aprender sobre cualquier protocolo y aplicación

GUARDIA FIREWALL SYSTEM DE NETGUARD

NetGuard es una compañía de software que se especializa en soluciones de seguridad para las redes corporativas en Internet. Guardian Firewall System, fue el primer firewall diseñado para operar en plataformas Windows NT y Microsoft.

FIREWALL DE RAPTOR

Fundada en 1992, Raptor Systems fue una de las compañías líderes en la integración del software y de los servicios para la seguridad de los firewalls. Hace poco, Raptor se fusionó con AXENT y ha fortalecido aún más su posición líder en el mercado de la seguridad para los firewalls y las redes

Raptor Firewall de AXENT contiene uno de los conjuntos más poderosos de aplicaciones proxy entre todos los firewalls con aplicaciones proxy que evaluamos. En muchos casos, inspeccionó los datos que viajaban por el firewall con mayor detenimiento de lo que lo hizo FireWall-1 de Check Point. Basada en la arquitectura de firewall de nivel de aplicación, la familia Eagle incluye una suite de componentes modulares de software que proporciona seguridad de red en tiempo real para Internet, para los grupos de trabajos, para la computación móvil y para los dominios de oficinas remotas dentro de una empresa

La familia Eagle, cuando se utiliza en forma individual o como parte de un sistema integrado de administración de seguridad para las redes, soluciona las necesidades de seguridad de red en

compañías grandes y pequeñas. Eagle se ejecuta en estaciones de trabajo de Sun Microsystems, Hewlett-Packard y Windows NT.

4.4. Reportes

Introducción

Los resultados del monitoreo pueden representarse en muy diversas formas; la más común de ellas es en un historial de resultados, aunque algunos equipos y software son capaces de entregarlos por medio de alertas visibles y audibles en el momento en que un evento ocurre en el sistema monitoreado. La información así obtenida no es un resultado, más bien es una herramienta que nos permite deducir el estado de la red o el equipo y decidir las medidas necesarias para resolver los problemas.

El mundo de la red permite generar reportes como:

- Los sitios más populares
- Los usuarios más activos
- Uso contra tiempo del día
- Uso contra tipo de tráfico (ejem. Web vs. FTP)
- Contenido de transferencias FTP y búsquedas
- Reportes que aportan costos a usuarios específicos, grupos o clientes
- SurfTime Meter y reportes que calculan exactamente cuánto está gastando una organización en tiempo de recreación
- Escritor Personalizado de Reportes el cual captura información en una base de datos compatible en tiempo real, entonces se pueden crear usuarios personalizados y reportes de estaciones de trabajo
- Alertas Activas, es decir, recibir alertas automáticas cuando ciertas políticas se violen, tales como tiempo perdido de surfing o tipo de sitio visitado

Tipos y usos

Los programas de monitoreo tanto operativo como de seguridad tienen diversas formas de entregar resultados, en base a los cuales se puede evaluar el desempeño de la red analizada o monitoreada

Estos resultados se obtienen desde tiempo real hasta registros semanales o mensuales dependiendo de la importancia de los datos obtenidos y de las necesidades de la organización, así por ejemplo si alguien desea saber el estatus de un servidor o una conexión determinada, puede saberlo en tiempo real o mediante un reporte semanal e incluso vía remota en un localizador o correo electrónico.

Básicamente existen dos tipos de reportes: Los gráficos y de texto.

- Los reportes elaborados en base a texto son capaces de mostrar una gran cantidad de información en un tamaño de archivo menor a los gráficos. Pueden ser enviados a puntos remotos para su lectura, resultan más rápidos y flexibles si se envían en texto, ya que así es posible verlos en equipos de comunicación portátil. La desventaja es que requieren un mayor tiempo para ser analizados e interpretados.

- El formato grafico permite observar el estado de la red o equipo de un sólo vistazo así como la evolución del evento, su tendencia e historial. Estas ventajas requieren de una mayor cantidad de recursos en el sistema o red y de dispositivos capaces de desplegar la información.

Otros programas crean sus reportes de manera automática y en formato "html" lo que permite que este reporte pueda ser revisado desde cualquier parte del mundo vía Internet, siempre y cuando este en un servidor con los servicios adecuados.

A continuación se muestran algunos tipos de reportes basados en el software de monitoreo BMC Patrol.

Este reporte está hecho en texto debido a la gran cantidad de información que maneja, además de emplear criterios de búsqueda, por ejemplo, en este caso se muestra el reporte de alarmas y alertas en una zona en específico así como el estatus de un servidor en particular.

List of Alerts

The following table lists the PATROL parameters that are in a WARNING or ALARM state. Click a parameter name to view the parameter definition information. Click a PATROL KM name to view the PATROL KM definition information. Click an application instance name to view detailed information about the instance. Click a host name to view detailed information about the monitored applications.

	Status	Parameter	Loaded PATROL KM	Instance	Host Name	Value	Border	Alarm 1	Alarm 2
	ALARM	[illegible]	NT_CPU	CPU_0	s2321	100	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2314	100	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2135	100	n/a	n/a	n/a
	WARN	[illegible]	NT_CPU	CPU_0	s2135	84.11	n/a	n/a	n/a
	WARN	[illegible]	NT_PAGEFILE	D__pagefile_sys	s2133	83.75	n/a	n/a	n/a
	ALARM	[illegible]	NT_SERVICES	Browser	s2116	0	n/a	n/a	n/a
	ALARM	[illegible]	NT_SERVICES	Browser	s2116	0	n/a	n/a	n/a
	ALARM	[illegible]	NT_PAGEFILE	D__pagefile_sys	s2108	95.6	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2125	98.95	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2117	100	n/a	n/a	n/a
	WARN	[illegible]	NT_CPU	CPU_0	s2125	81.7	n/a	n/a	n/a
	WARN	[illegible]	NT_CPU	CPU_0	s2117	84.8	n/a	n/a	n/a
	ALARM	[illegible]	NT_SERVICES	MSFTPSVC	s2028	10	n/a	n/a	n/a
	ALARM	[illegible]	NT_SERVICES	MSFTPSVC	s2028	10	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2113	100	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2043	100	n/a	n/a	n/a
	ALARM	[illegible]	NT_CPU	CPU_0	s2043	95.19	n/a	n/a	n/a

Host Details

The following table provides detailed information about the host . Click a PATROL KM name to view the PATROL KM definition information. Click an application instance name to view the runtime parameter information. Click the event history icon for a host to view the history of events generated by the PATROL Agent.

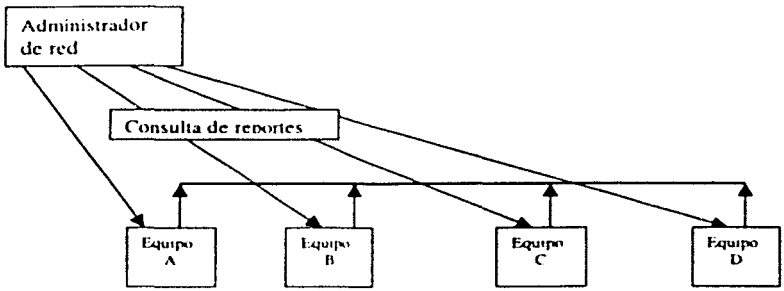
	Loaded PATROL KM	Instance	Status	Details
	NT	nt_local	OK	Events
	PATROL_NT	PATROL_NT	OK	Events
	NT_SERVICES_CONTAINER	NT_SERVICES_CONTAINER	OK	Events
	NT_SERVICES	Alerter	OK	Events
	"	EventSystem	OFFLINE	Events
	"	ClipSrv	OFFLINE	Events
	"	Browser	OK	Events
	"	DHCP	OFFLINE	Events
	"	Replicator	OFFLINE	Events
	"	EventLog	OK	Events
	"	MSFTPSVC	OK	Events
	"	IISADMIN	OK	Events
	"	LicenseService	OK	Events
	"	MSDTC	OK	Events
	"	Messenger	OFFLINE	Events
	"	DNS	OK	Events
	"	NtLmSsp	OK	Events
	"	Netlogon	OFFLINE	Events
	"	NetDDEdsdm	OFFLINE	Events
	"	NetDDE	OFFLINE	Events
	"	albservice	OK	Events
	"	PatrolEvMonitor	OK	Events
	"	PatrolProcessMonitor	OK	Events
	"	PatrolAgent	OK	Events
	"	RTTsvc	OK	Events
	"	PlugPlay	OK	Events
	"	ProtectedStorage	OK	Events
	"	RPCLOCATOR	OFFLINE	Events
	"	RpcSs	OK	Events
	"	SNMP	OK	Events
	"	SNMPTRAP	OFFLINE	Events
	"	LanmanServer	OK	Events
	"	SimpTcp	OK	Events
	"	Spooler	OK	Events
	"	SENS	OFFLINE	Events
	"	Lmhosts	OK	Events

Debido a las limitantes de la red y al porcentaje de recursos que se reservan para el monitoreo, es necesario implementar acciones que lo hagan más eficiente como por ejemplo un monitoreo selectivo y oportuno o uno escalonado, es decir que sólo se verifiquen los datos que son realmente importantes y con la frecuencia adecuada o que sólo si se cumplen determinadas condiciones el monitoreo avanzará a una fase que consuma una mayor cantidad de recursos.

El objeto de planear la requisición de reportes permite tener la mayor cantidad de recursos libres en el momento en que más se necesitan, sin que el monitoreo se convierta en una carga excesiva en la red, permitiendo así planear los horarios de mantenimiento preventivo y correctivo o el diseño de un proceso automático.

Otro aspecto a considerar en los reportes es la fiabilidad de los resultados que proporciona el sistema de monitoreo. Existen diversas estructuras de reporte y notificación las cuales se analizan a continuación:

MODELO A



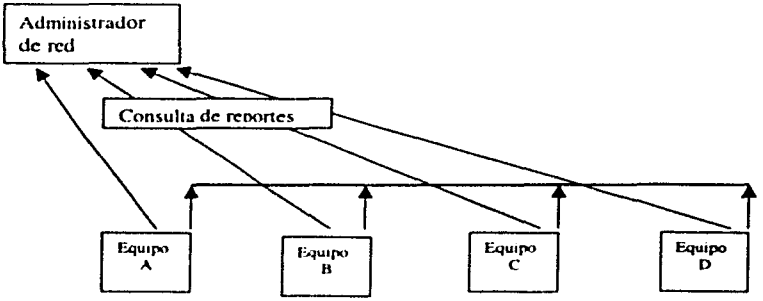
Ventajas

- La información se obtiene de primera mano.
- Si algo está mal se puede observar desde la primera vez que se intenta obtener el reporte.
- No se utiliza la red para obtener el reporte así que este no puede ser modificado mentras viaja por un medio poco fiable.

Desventajas

- Hay que conectarse equipo por equipo.
- No existe un reporte unico que permita decidir si la infraestructura completa está funcionando.

MODELO B



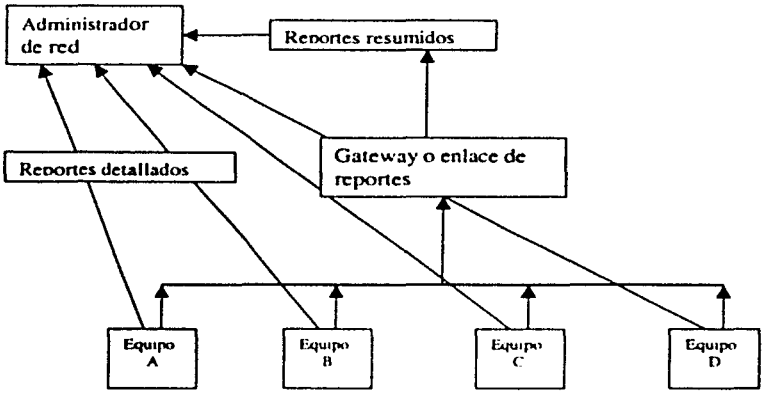
Ventajas

- La información se obtiene de forma centralizada y de toda la infraestructura.
- Se observa fácilmente si un equipo deja de reportar.

Desventajas

- Se tiene que revisar reporte por reporte para determinar las fallas.
- Se hace uso de la red la cual no es 100% confiable.
- El proceso de notificación usando gateways impacta en el tiempo de respuesta.

MODELO C



Ventajas

- El administrador obtiene un solo estado de toda la infraestructura
- Obtiene los resúmenes y si es necesario existe un reporte detallado
- Se detecta fácilmente si un equipo deja de reportar
- Se pueden asignar distintos gateways a distintos administradores según sea necesario

Desventajas

- Tanto los reportes como las notificaciones se obtienen en cada gateway así que se repiten.
- El uso de gateways impacta en el tiempo de respuesta

Análisis de resultados.

Así como es necesario determinar las condiciones y capacidades de la red al implementar el sistema de monitoreo, se requiere también analizar esta misma información al momento de

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

obtener los primeros resultados del monitoreo. Los reportes obtenidos no pueden ser considerados como resultados finales en sí mismos, sino que tendrán un significado distinto en redes distintas. Debido a que básicamente el monitoreo funcional se enfoca a preservar el desempeño de la red y el monitoreo de seguridad a mantener la privacidad e integridad de los datos, estos son los aspectos más importantes a considerar en el diseño de los reportes de monitoreo.

Por otro lado resultaría prácticamente inútil implementar un sistema de monitoreo en una red que no tiene una estructura o un orden mínimo; por sentido común el primer paso en la implementación del monitoreo es la revisión del estado físico de la red (esto claro, a nivel red local del proveedor del servicio) ya que por lo general un usuario a nivel Internet no tiene control más allá de su terminal. Una vez validado el correcto funcionamiento de los equipos de la red, puede procederse a un estudio de la estructura, tales como el análisis del porcentaje de uso de procesadores, memoria libre, espacio en disco duro y tiempos de respuesta en servidores, dicho análisis nos proveerá de la información necesaria para determinar los cuellos de botella en el proceso.

El tiempo de respuesta en el sistema, es un indicador del desempeño de la red. Considerando que la aplicación se está utilizando vía Internet, hay que tomar en cuenta la diversidad de medios por los que los datos son enviados a la central de procesamiento y se devuelven al usuario final. La velocidad puede verse afectada por elementos como el tipo de conexión del usuario a los servicios de Internet, la capacidad del servidor de Internet, el proceso de enlace y autentificación del usuario, el acceso satelital del proveedor de Internet, así como la cantidad de solicitudes de servicio y de datos recibidos por el proveedor.

Después de los resultados obtenidos en el monitoreo preliminar, el siguiente paso es la determinación de las características de la red así como las exigencias mínimas requeridas por la Organización. Una vez obtenidos estos datos se inicia la comparación entre lo existente y lo requerido para establecer:

- Políticas de Seguridad.
- Prioridades de Acceso a los servicios vía Internet, Intranet y Extranet.
- Umbrales de alerta.
- Umbrales de alarma.
- Programación de mantenimientos preventivos y correctivos.
- Creación de bitácoras que permiten el establecimiento de tendencias.

Finalmente, la continuidad en el análisis de los reportes nos permitirá detectar, analizar, informar y diagnosticar eventos y estados en los Sistemas y Aplicaciones que proporcione las causas y ayude a la búsqueda de soluciones.

CONCLUSIONES

CONCLUSIONES

Después del estudio de los elementos de cada una de las fases que componen una red, es evidente que cada componente en la red influye en el desempeño de los procesos de negocio de las empresas, ya que además de ser un medio de comunicación con los clientes y un canal de ventas, representa el eje del modelo operativo actual.

El desarrollo de una red exitosa de cualquier tipo depende de varios factores. Es de suma importancia tener muy claro el alcance de la red, es decir que se busca en la red; si se busca reducir costos, si aumentar la eficiencia, si incrementar ventas o hacer mas eficiente el canal de distribución, las tecnologías existentes en el mercado, el costo de implementación y los factores de riesgo en la seguridad de los recursos y aplicaciones.

Para mantener la ventaja o el valor agregado de la empresa es necesario desarrollar una estrategia que permita subsanar deficiencias o cubrir las necesidades de los usuarios, es decir comprobar que la red soporte los procesos operativos de la empresa para mantener la calidad del servicio y el nivel de eficiencia. Esta estrategia debe contemplar el monitoreo como parte fundamental en el óptimo desempeño de la red.

El monitoreo de una red permite programar un aumento de capacidad que será necesario en un tiempo determinado, ya que un crecimiento demasiado rápido no es recomendado y esperar tanto podría tener una respuesta mala o que el servicio sea interrumpido.

Por este motivo es importante que en la constitución física de la red se considere:

- Capacidad de crecimiento a bajo costo.
- Base para soportar todas las tecnologías de niveles superiores.
- Realizar una instalación compatible con las tecnologías actuales y las que estén por llegar.
- Tener la suficiente flexibilidad para realizar adecuaciones a las necesidades de las personas y recursos dentro de la instalación.
- Estar diseñada e instalada de tal manera que permita una fácil supervisión, mantenimiento y administración, es decir, que sea fácilmente gestionable y fiable, lo que se traduce en un mejor control del ambiente

El monitoreo ayuda a desarrollar escenarios a largo plazo con un nivel de servicio estable y que el cliente quede satisfecho. Cuando las cargas de trabajo crecen sobre el tiempo, las bitácoras de monitoreo pueden ayudar a modelar el sistema de resultados y el tiempo de respuesta.

Por medio del monitoreo se puede identificar la capacidad instalada que no se utiliza, permitiendo a través del análisis modelar una distribución balanceada al sistema. Esto permite

evaluar la necesidad de recursos para obtener más capacidad y ayudar a resolver problemas funcionales rápidamente minimizando los gastos.

Ahora bien las consideraciones que se deben tener presentes en la toma de decisiones, para la implementación de un software o hardware de monitoreo se resumen en:

1. Se debe tener presente que el monitoreo de la funcionalidad y seguridad de la red cuesta, por lo que se debe evaluar el impacto de las aplicaciones fuera de línea así como los dispositivos desconectados, es decir realizar un análisis de costo – beneficio, en donde demos respuesta a las siguientes preguntas:

- ¿Qué impacto tiene la aplicación si está fuera de línea?
- ¿Cuánto tiempo puede estar sin los dispositivos desconectados?
- ¿Cuál es el % de riesgo del Sistema de Monitoreo?

2. Los acuerdos de nivel de servicio así como los acuerdos de nivel de seguridad deberán estar apoyados por las políticas de seguridad establecidas de antemano por la empresa, mismas que están destinadas a controlar la estabilidad del ambiente. Por ejemplo, se debe especificar cuanto tiempo en promedio puede estar fuera la red sin que afecte los criterios de disponibilidad de las mismas.

3. Delimitar la red, se debe conocer el perímetro de la red y como vamos a interactuar con los administradores, es decir, ¿Quien administra el enlace satelital y cual es su nivel de servicio? o ¿Cuanto tiempo (%) puede estar abajo el enlace que brinda un proveedor de servicios de enlaces de telecomunicaciones?

4. Seguridad en tránsito, mantener seguridad mientras la información viaja a través de la red. Se debe cuidar que:

   - Nadie intercepte la información para ser mal uso de esta o introduzca datos falsos.
   - Disponibilidad del medio y el servicio.
   - El tiempo en que tarda la información en llegar, sea útil y responda a las necesidades del usuario.

5. Seguridad en el Host, seguridad en el almacenamiento, procedimiento para respaldo de información, seguridad a nivel usuario final.

6. La determinación de un software estará basada en cargas de trabajo que están compuestas por los usuarios y recursos del sistema que requiere llevar a cabo un proceso comercial.

Algunos productos de software de monitoreo analizan y modelan las herramientas de ambientes UNIX, Windows, Mac o bases de datos como Oracle, Sybase, Informix y SAP R/3. Cuando se

implementan aplicaciones críticas en un negocio, el impacto de las mismas sobre el sistema debe ser óptimo, pero no siempre resulta un desarrollo factible.

También es importante resaltar que los canales de transmisión son fundamentales en la construcción de la red, pues determinan el límite de velocidad de ésta. Aunque existen muchos tipos de cables, antenas, etc. al estandarizar las instalaciones físicas se ha limitado, por sentido común, la utilización de dos tipos de medios de comunicación: el par trenzado en cobre y la fibra óptica.

Ahora bien, con el monitoreo en la red, se puede determinar si la configuración propuesta es adecuada para la demanda esperada o si un cambio en el diseño de aplicación será requerido, se puede justificar compras de hardware o software y demostrar el tiempo correcto de mejora así como las consecuencias de no hacerlo en el momento.

Las técnicas avanzadas de monitoreo que el mercado ofrecen la capacidad para predecir el punto en el cual el servicio se vuelve inaceptable, así pues las mejoras pueden ser programadas para mantener un nivel de servicio competitivo. También pueden determinar el tiempo de respuesta y su tendencia, ayudando a anticipar e identificar cuellos de botella y eliminarlos rápidamente.

Los resultados del monitoreo que nos permiten analizar la situación de la red, encontrar problemas e identificar sus causas son los reportes. Es común que dichos reportes provean información utilizando códigos de color que proporcionen información vital rápidamente. Una vez que el problema es identificado permite a los administradores gestionar soluciones potenciales sin afectar el desarrollo del sistema. Esto permite comparar soluciones y seleccionar el mas adecuado para restablecer la funcionalidad del sistema.

Para un monitoreo correcto, se requiere determinar el impacto de los cambios del negocio sobre el sistema; es importante mantener bitácoras de los reportes proporcionados por el software de monitoreo los cuales nos ayudar a resolver incognitas como.

En resumen un monitoreo adecuado permite:

- Reforzar el control del ambiente para alcanzar el cumplimiento de las metas en el nivel de servicio.
- Eliminar interrupciones a los procesos de negocio criticos.
- Reforzar la deteccion de eventos que afectan la disponibilidad del sistema así como proporcionar la informacion para implantar mejoras.
- Identificar problemas utilizando reportes que ayudan a comprender los problemas y tendencias a desarrollar. Un reporte del nivel del servicio entrega un cuadro completo de eventos y el estado de los sistemas y aplicaciones, un análisis grafico da una visión de los problemas identificando sus causas para proponer soluciones.

- Satisfacer necesidades del cliente por contar con un sistema de apoyo eficaz y confiable de la aplicación.

En cuanto al análisis de seguridad, los datos filtrados ahorran tiempo y mejoran la productividad por las ventajas que representa el anticipar puntos de falla en vez de esperar a corregir consecuencias y las causas mismas; permitiéndoles a los gerentes del sistema enfocar la información más crítica. Pueden definirse y condicionarse umbrales para la métrica del sistema donde notifica y recomienda las acciones correctivas anticipándose a las consecuencias negativas que puedan ocurrir.

Con respecto al acceso desde el interior de una LAN hacia el exterior, podemos decir que, si desde cualquier estación enviamos un paquete a un dispositivo y el Firewall nos valida el tamaño, IP de destino, puerto, etc. (estos parámetros varían según las necesidades de seguridad de cada red, y por ende, del nivel de configuración del Firewall), el usuario autorizado no notará ninguna diferencia entre la existencia o no de la barrera.

En conclusión, las herramientas que actualmente nos presenta el mercado ofrecen una amplia gama de soluciones que permiten satisfacer las necesidades específicas de cada negocio.

La clave para una correcta implementación de un sistema de monitoreo, está en la elección de un software y/o hardware acorde a los requerimientos y recursos disponibles en la empresa.

GLOSARIO

GLOSARIO

Acceso Remoto Comunicación con una computadora a través de terminales que están distantes.

Algoritmo Un conjunto finito de reglas que dan una secuencia de operaciones para solucionar un problema específico.

Apantallado Recubrimiento del cable, ya sea de papel aluminio o malla de cobre.

ARPANET Advanced Research Projects Agency Network. Red de la Agencia de Proyectos de Investigación Avanzada Norteamericana a través de líneas telefónicas de la que posteriormente derivó Internet.

Asíncrono Término referido a las comunicaciones. Uno de los componentes esenciales de una computadora es el reloj. Pues bien, cuando en el traspaso de información entre computadoras no se utilizan mecanismos de sincronización mediante los relojes, sino que por cada caracter o conjunto de ellos se han de transmitir señales para asegurar la correcta transmisión, se dice que esta es asíncrona.

Ataques Entrada no autorizada al sistema.

Atenuación Disminución o perdida de una señal.

ATM Asyncronous Transmision Mode. Modo de Transmisión Asíncrona. Sistema de conmutacion de paquetes en banda ancha que soporta velocidades hasta 1.2 Gbps.

Autentificación Consiste en validar que la identidad del usuario sea la que él reclama.

Autorización de Acceso Dar permiso a un objeto (persona, terminal o programa) para ejecutar un conjunto de operaciones en el sistema.

Base de Datos Una coleccion no redundante de datos interrelacionados, procesables por una o mas aplicaciones.

Bit Binary Digit. Unidad mínima de información utilizable por una computadora. Teniendo en cuenta que el funcionamiento es por medio del sistema binario, los únicos valores que puede contener un bit son el 0 y 1.

Bridge Puente. Dispositivo que conecta dos segmentos de una red y pasa paquetes entre ellos.

Byte Octeto es español. Es la unidad mínima de información, y está compuesta por ocho bits.

Callback Es un método desarrollado para identificar una terminal que trata de conectarse a un sistema de computo, desconectando la terminal que llama y restableciendo la conexión con el sistema de computo.

CCITT Comité Consultivo Internacional de Telegrafía y Telefonía. Organismo internacional que desarrolla estándares de comunicaciones, como la recomendación X.25.

Codec Es un aparato que convierte la señal analógica en digital y viceversa.

Código Método de cifrado por sustitución. Un código pone en clave una sola unidad lingüística de longitud variable, que típicamente viene a ser una palabra o frase.

Confidencial Una clasificación de datos, de los cuales el uso o divulgación no autorizados podría causar daño serio a una organización.

Control de Acceso Tareas llevadas a cabo por hardware, software y controles administrativos para monitorear la operación de un sistema, asegurar la integridad de datos, hacer la identificación del usuario, grabar accesos y cambios al sistema, y dar acceso a los usuarios autorizados.

Cookies Si bien se utilizan teóricamente en un sentido publicitario en forma de una ventana, en realidad son conexiones del servidor al cliente, capaces de almacenar datos de cada usuario. Es uno de los sistemas característicos de almacenamiento de información privada por parte de determinadas empresas.

Cortafuegos Firewall. Sistema típico que se utiliza para evitar la entrada en las computadoras de personas no deseadas. Hay distintos sistemas, pero en definitiva lo que hacen es controlar el tráfico que se está produciendo en la red. Es utilizado mayormente en las Intranets para que cualquier mensaje que entre o salga de la misma pase primero por él, que examina cada uno de ellos y bloquea los que no cumplen con los criterios de seguridad impuestos.

Cracker Persona especializada en la desprotección de programas, dejándolos sensibles a la copia.

Criptoanálisis Desbaratar las cifras.

Criptografía El arte de crear claves.

Criptología Nombre colectivo para designar a la criptografía y al criptoanálisis.

Checksum Un bloque de longitud fija producido como una función de cada bit en un mensaje encriptado. Una suma de un conjunto de datos para detectar errores.

Datagrama Usualmente se refiere a la estructura interna de un paquete de datos.

Datos Termino general relativo a numeros, letras, simbolos y cantidades.

DHCP Dinamic Host Configuration Protocol. Servicio que asigna direcciones IP de forma dinámica en una red

Dispersión de la Luz Es la separación de la luz en diferentes longitudes de onda.

DoD Departamento de defensa de Estados Unidos.

Duplex Expresión que se utiliza cuando la transmisión de datos puede efectuarse en ambas direcciones. Cuando el medio utilizado permite la comunicación en los dos sentidos (emisor-receptor y a la inversa), pero no al mismo tiempo, se trata de Half Duplex. Si se puede producir al mismo tiempo es Full Duplex.

Ethernet Tipo de red muy estandarizada cuyo desarrollo inicial corresponde a Xerox. Su Topología es en bus (no confundir con el concepto Bus como "canales" internos a la computadora). Puede alcanzar velocidades entre 1 y 20 Mbps (megabits por segundo), aunque es normal los 10 Mbps utilizando banda base. Se monta sobre cable coaxial.

Extranet Al igual que Intranet, son "hermanos menores" de Internet, es decir, que se utilizan los mismos protocolos, sistemas de páginas www, pero en este caso sirven para unir sectores más amplios que las anteriores, como distintas empresas.

FDDI Fiber Distributed Data Interfaz. Es un estandar para redes de alta velocidad

Fibra Óptica Tipo de cableado para comunicaciones. En transmisiones por cable son utilizadas las de cobre o éstas, que sustituyen el metal por el vidrio o producto similar que deje pasar la luz con un mínimo de impurezas, y que se van imponiendo poco a poco. La transmisión no se efectúa por impulsos eléctricos sino luminosos. A excepción de los problemas de empalmes o codos e incluso curvaturas que pueden entorpecer la propagación y de los surgidos por la conversión de los impulsos eléctricos de las computadoras a luminosos las ventajas son muy grandes: el ancho de banda es mucho más alto, el diametro del cable es muy fino, las interferencias

	electromagnéticas, por maquinarias, etc. no afectan, es más seguro, y sus precios tienden a ir bajando.
Frame Relay	Es un sistema de transmisión de datos que utiliza tramas (frames, bloques de información delimitados) y no paquetes. Permite altas velocidades y tráfico, incluyendo voz y datos (servicios Frame Relay - Data Voz).
FTP	File transfer Protocol. Se utiliza para transferencia de archivos.
Gateway	Compuerta o servidor de intercomunicación. Se refiere a un dispositivo de propósito especial que efectúa una conversión de información de nivel de capa 7 de una pila de protocolos a otra.
Hacker	Persona que intenta tener acceso no autorizado a computadoras. Generalmente lo hace por el reto intelectual y el desafío tecnológico que esto implica.
HDLC	High-level Data Link Control.
Homologar	Hacer pruebas respecto a la calidad de un producto para comprobar si se ajusta a determinadas normas.
Host	Computadora conectada a Internet. Computadora en general. Literalmente anfitrión.
HTTP	Hypertext Transfer Protocol.
Hub	Concentrador. Termino que describe un dispositivo que sirve como centro de una red con topología estrella. Pueden ser activos (que repitan la señal que les llega) o pasivos (que no repiten, sólo reparten las señales).
Identificación de Usuario	Característica única (tarjeta, número, etc.) que sirve para conocer la identidad de un usuario.
IDU	Interface Data Unit.
IEEE	Institute of Electrical and Electronics Engineers. Organismo internacional que desarrolla estándares en el área de ingeniería eléctrica e informática.
Índice de Refracción	Es el grado de propagación de un haz luminoso a través de un cierto material.
Información	Datos colectados y presentados de forma que contengan un significado.

Integridad de datos Es estado en el que los datos son los mismos que en los documentos fuente y no han sido expuestos a alteración o destrucción maliciosa o accidental.

Interfaz Él limite entre dos cosas, por lo general dos programas, dos piezas de hardware, una computadora y su usuario, etc.

Interferencias Electromagnéticas Frecuencias externas que provoca distorsión en una señal.

Internet Seguro que es el término más popular en estos momentos cada vez que se habla de informática en general. Se le pueden dar definiciones puntuales, como "red de redes" que aunque no nos sirve para entender nada, está bien, pues en definitiva no es más que redes de computadoras interconectadas.

Intranet Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo *TCP/IP* y servicios similares como *WWW*.

ISO International Organitation for Standardization. Organismo Internacional para la Estandarización. Es responsable de una amplia gama de estándares, incluyendo aquellos relevantes para las redes.

LAN Red de Área Local. Red que cubre un área geográfica relativamente pequeña. Comparadas con las redes WAN, suelen caracterizarse por velocidades de transferencia de datos relativamente altas y baja incidencia de errores.

LAP-B Link Access Procedure-Balanced.

Luz Coherente Los fotones están ordenados uniformemente.

Módem Contracción de Modulador-Demodulador. Dispositivo para comunicación de computadoras a través de línea telefónica. Cuando transmite el modem convierte señales digitales en analógicas, y cuando recibe hace el proceso inverso.

NJE Network Job Entry

OSI Modelo de referencia OSI (Open System Interconnection). Modelo de arquitectura de redes desarrollado por ISO y CCITT. Este modelo es universalmente usado como método para enseñar y entender la funcionalidad de las redes.

Paquete La información en la red en general no se transmite en un bloque, sino fragmentada. Cada uno de estos fragmentos se denomina

	paquete, e incluye información del destino y la necesaria para que puedan ser "reorganizados" a su llegada.
Password	Contraseña. Cadena de caracteres privada que sirve para verificar que la identidad de un usuario sea verdadera.
PDU	Protocolo Data Unit.
Ping	Comando de prueba de comunicación
Política de Seguridad	El grupo de reglas y regulaciones que dicta como una organización protege, maneja y distribuye información sensible.
Polling	Sondeo que realiza el servidor para comprobar el estado de cada terminal en una red.
Procedimientos de respaldo(Backup)	Métodos usados para recuperar informacion en una computadora después de un desastre o falla del sistema.
Protocolo	Es un término de comunicaciones y su función es fijar unas reglas de funcionamiento, a todos los niveles, a las que han de atenerse los distintos sistemas informáticos para poder comprenderse.
Proxy	Utilizado en las redes de area local, un proxy es un servidor virtual que realiza la conexion con el servidor real de Internet y a través del cual se conectan el resto de las computadoras clientes.
Recurso	Cualquier cosa usada o consumida mientras se realiza una función.
Router(Enrutador)	Se denomina así al dispositivo capaz de dirigir la información, dividida en paquetes, por el camino más idoneo, examinando la direccion y el destino y utilizando mapas de red.
SAP	Service Access Points.
Seguridad de Datos	Proteger los datos contra modificacion destrucción o divulgación.
Seguridad en Redes	Medidas para proteger una red de acceso no autorizado, interferencia accidental o intencional, daño a instalaciones fisicas o software.
Site	Lugar o "sitio" donde esta instalado, o puede ser instalado cierto equipo de computo.
SMTP	Simple Mail Transfer Protocol. Es una aplicacion para correo electronico.
SNA	Sistems Network Architecture.

Sniffers	Sistemas de espionaje o robo de información, gracias a la "captura" de los paquetes que pasan por los servidores, aunque la dirección de destino sea otra.
SNMP	Simple Network Management Protocol. Se trata de una aplicación para el control de la red
Software de Aplicación	Un programa o grupo de programas que dice a la computadora cómo hacer trabajos específicos
TCP/IP	Transmission Control Protocol-Internet Protocol. Protocolo en el que se basa Internet y que en realidad consiste en dos. El TCP, especializado en fragmentar y recomponer paquetes, e IP para direccionarlos hasta su destino
Telemática	Conjunto de técnicas y servicios basados en redes que asocian la telecomunicación y la informática
Telnet	Protocolo mediante el cual se puede realizar una conexión a servidores basados en UNIX
Token Ring	Sistema de red de área local creado por IBM. Se basa en una topología de bus en anillo y paso de testigo
Trap Door	Es un conjunto de instrucciones que permiten a un usuario traspasar las medidas estándares de seguridad de un sistema
UNIX	Sistema Operativo desarrollado por AT&T en 1969 en lenguaje ensamblador, posteriormente se rescribió a lenguaje C lo que ha hecho posible su desarrollo actual. Es quizás el S.O. más extendido entre computadoras de tamaño medio. De él han surgido distintos sistemas derivados como lo fue Xinux o el actual Linux
UPS	Sistema ininterrumpido de suministro de electricidad. Provee protección al equipo de procesamiento de información contra suspensión de energía eléctrica, bajas de voltaje, picos de corriente y ruido eléctrico.
Vulnerabilidad	Susceptibilidad de un sistema a una amenaza de ataque específico o evento dañino

BIBLIOGRAFÍA

BIBLIOGRAFÍA.

Guía práctica de comunicaciones y redes locales.
Antonio Cebrián Ruz, Eduardo Borraz Faci.
Ed. Gustavo Gili, S.A., 1993

Redes de computadoras
Andrew S. Tanenbaum
Ed. Prentice Hall, 1991

Artículo : "Organización básica en redes locales"
David Matas
PC WORLD, Marzo 1996

Sistemas para la transmisión de datos
Fernando Torres Medina
Secretariado de publicaciones, Universidad de Alicante, 1996

Data Communications, Computer Networks and Open Systems
F. Halsall
Editorial Addison-Wesley , 1992

Las redes de empresa
P. Bichon, P. Gomez
Ed. Gestión 2000 S.A., 1994

Teleinformática y redes de computadoras
Ed. Marcombo S.A.
Revista CHIP
Enero 1991

PC MAGAZINE nº 64

RED n° 137

High-Performance Communication Networks
J. Walrand, Pravin Varaiya
Ed. Morgan Kaufmann Publishers
2da. Edición.
2000

Comunicación de datos, redes de computadoras y sistemas abiertos
Fred Halsall.
Ed. Pearson Education
4ta. Edición.

Todo acerca de redes de computación
Kevin Stoltz
Ed. Prentice-Hall

Seguridad de la Información en sistemas de cómputo
Luis A. Rodríguez
Ed. Ventura
1995

Señales y Sistemas.
Alan V. Oppenheim
Alans Willsky
Ed. Prentice Hall
2a. Edición
1998