1 Temario

2 Introducción

La industria de la computación es relativamente joven, comparada con otras industrias, aún en el área de telecomunicaciones, como por ejemplo la telefonía. Sin embargo, la rapidez de crecimiento y el abaratamiento de costos hace que hoy en día las computadoras están al alcance de la gran mayoría de las personas y de prácticamente todas las empresas.

Junto con la proliferación de computadoras, surgió la necesidad de interconectarlas, para poder intercambiar, almacenar y procesar información.

Las redes de datos, tiene como objetivos

- Compartir recursos, equipos, información y programas que se encuentran localmente o dispersos geográficamente.
- Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- Obtener una buena relación costo / beneficio
- Transmitir información entre usuarios distantes de la manera más rápida y eficiente posible

La topología en las redes de datos puede ser enmarcada en dos tipos según el tipo de transmisión utilizada:

- **Redes de difusión**: Donde se comparte el mismo medio de transmisión entre todos los integrantes de la red. Cada mensaje (típicamente llamado "paquete") emitido por una máquina es recibido por todas las otras máquinas de la misma red. Cada paquete dispone de la información de "Origen" y "Destino" y de esta manera se discrimina quien debe procesar cada mensaje. Por ejemplo, Ethernet es una red de difusión

- **Redes punto a punto**: Donde existen muchas conexiones entre pares individuales de máquinas. Para enviar mensajes hasta máquinas distantes, puede ser necesario pasar por varias máquinas intermedias. Por ejemplo, las conexiones por MODEM son redes punto a punto.

En forma independiente la tecnología utilizada, las redes de datos pueden ser clasificadas en dos categorías, según el alcance o tamaño de las mismas:

- **LAN (Local Area Networks, Redes de Área Local):** Las redes LAN son de alcance limitado. Generalmente son redes privadas que están

instaladas dentro de un mismo edificio, oficina o campus. Su objetivo principal típicamente es compartir recursos (impresoras, discos, etc.).

Estas redes pueden tener velocidades de transmisión de hasta 1000 Mb/s y pueden tener topologías del tipo bus, estrella o anillo.

- **WAN (Wide Area Networks, Redes de Área Amplia):** Estas redes se extienden en una amplia zona geográfica, la que eventualmente puede ser dividida en subredes interconectadas con equipos de conversión de interfases y/o protocolos. Estos equipos se conectan con diferentes tipos de líneas de transmisión.

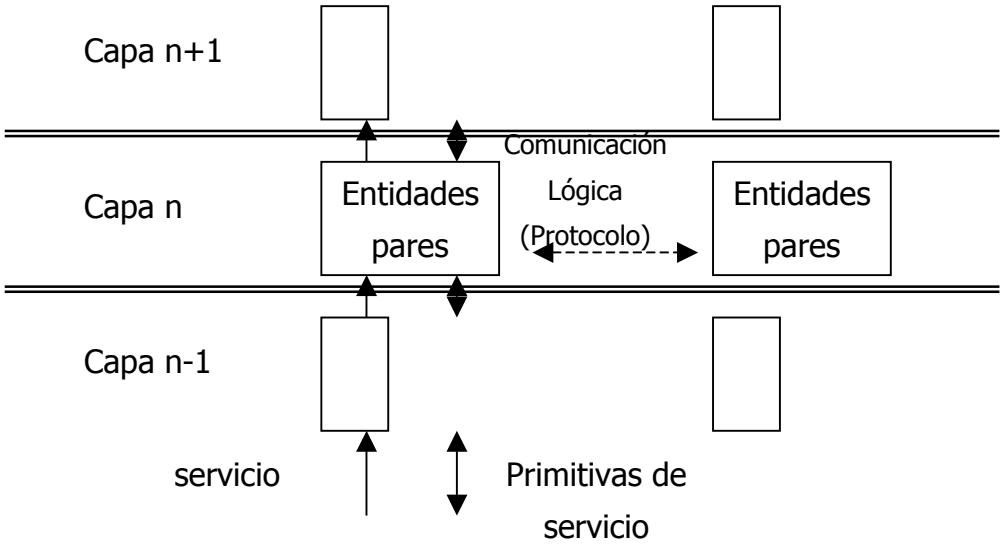
  Una de las funciones típicas de las redes WAN es la interconexión de dos o varias redes LAN.

  La topología de las redes WAN puede ser del tipo estrella, anillo, árbol o malla.

Algunos textos incluyen un tercer tipo de redes, las llamadas MAN (Metropolitan Area Network, Redes de área metropolitana). Dado que estas redes pueden asemajerse a las LAN o WAN (según cada caso), no las estudiaremos en forma independiente.

Todos los tipos de redes e interredes vistas anteriormente requieren de programas dedicados al control, mantenimiento y diseño así como sus conexiones.

Para reducir la complejidad del diseño, la mayoría de las redes están organizadas en “niveles” o “capas”. El propósito de cada capa es ofrecerle servicios a su capa inmediatamente superior. Cada capa se comunica con su similar en otra máquina, mediante reglas bien establecidas, llamadas “protocolos”. Esta comunicación se realiza a través de las capas inferiores, como se observa en la figura.



Cada capa tiene sus propias interfases, hacia las capas superiores e inferiores. Estas deben ser bien definidas para poder intercambiar información de un nivel a otro.

Un conjunto de capas y protocolos se denomina “arquitectura de red”. Actualmente existen muchas arquitecturas de red, entre las que figuran OSI, TCP/IP, SNA, etc. La mayoría de los protocolos y funciones de las capas de una arquitectura están desarrolladas en software (programas) pero últimamente se están desarrollando muchos protocolos, interfases y funciones, en hardware (equipos) y/o firmware (equipos programables).

Las capas de una arquitectura pueden ofrecer dos tipos de servicios: orientados a conexión y no orientados a conexión.

- **Servicios orientados a la conexión:** Son muy similares a los servicios de telefonía, donde se establece una conexión marcando un número determinado. Una vez establecida la conexión, se puede intercambiar información en forma segura y ordenada. Luego de terminado el intercambio de información, puede liberarse la conexión.
- **Servicios no orientados a la conexión:** Toman su modelo del servicio de correos, donde el mensaje es enviado sin establecer previamente una conexión entre origen y destino. Cada mensaje debe contener la dirección completa de su destino. Dos mensajes enviados al mismo destino (dos cartas, en el ejemplo), pueden viajar por caminos completamente diferentes antes de llegar al destino, e incluso puede suceder que el mensaje enviado en segundo lugar llegue a destino antes que el enviado en primer lugar.

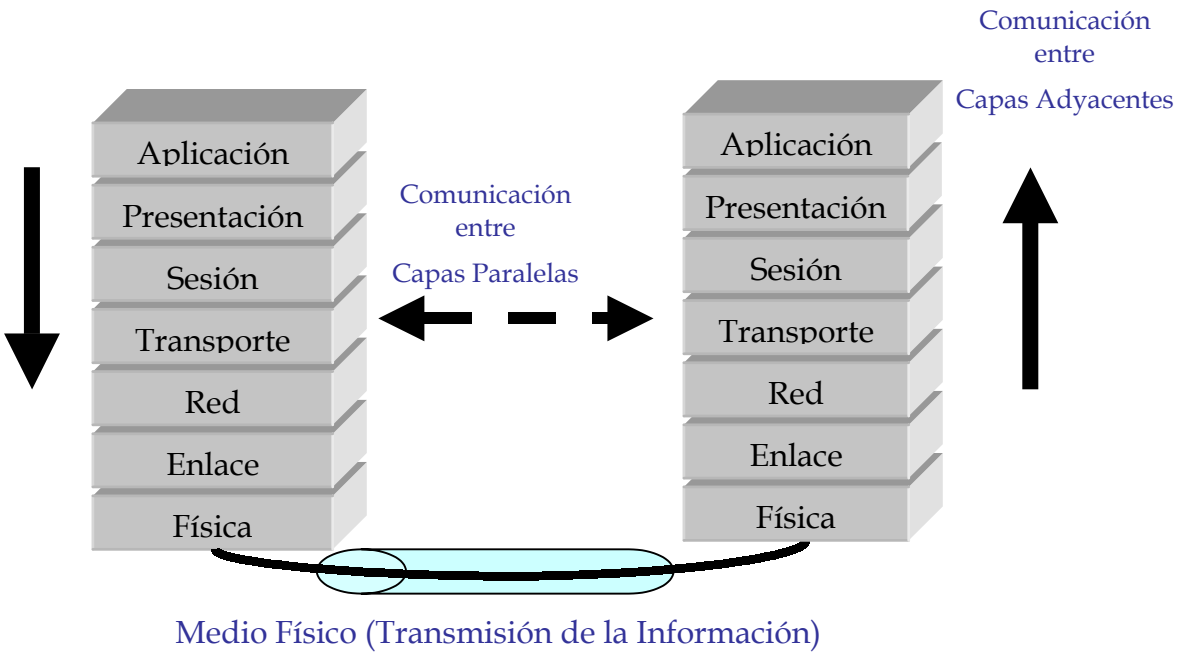
Una discusión más detallada acerca de los tipos de redes y los modelos de capas puede leerse en “Redes de Computadoras” de A. S. Tanenbaum [1]

3 Modelos de referencia OSI y TCP/IP

Como se vio en la introducción, la estructura de red se basa en modelos de capas, interfaces y protocolos.

Muchas arquitecturas basadas en capas partieron del modelo de referencia OSI y a partir de éste se generaron muchas otras arquitecturas como TCP/ IP y B-ISDN.

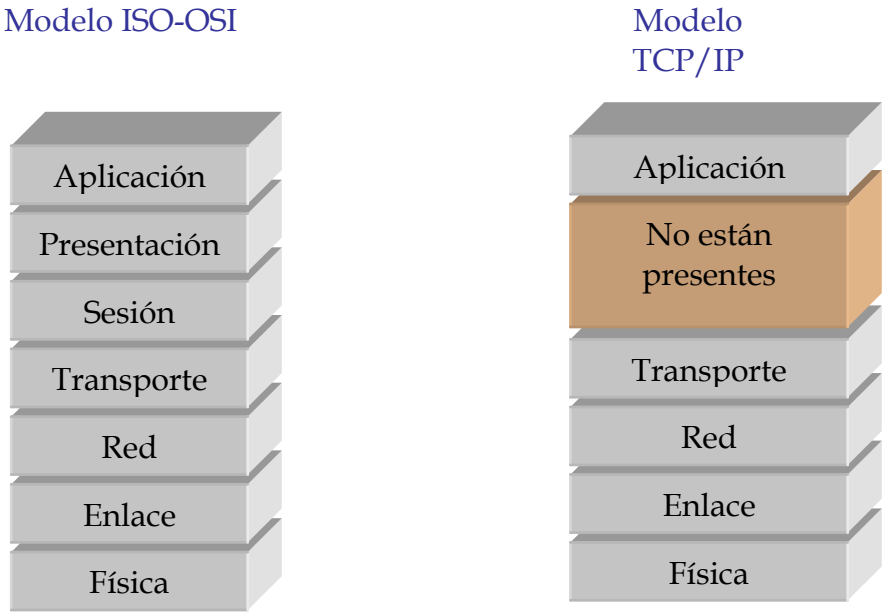
El modelo de referencia OSI (Open Systems Interconnection, Interconexión de Sistemas Abiertos) es un modelo de siete capas desarrollado por la Organización Internacional de Normas (ISO). En la figura se describe el modelo de capas de OSI.



Sobre la base del modelo de referencia OSI se desarrollaron otros modelos de red y arquitecturas completas para las redes de comunicación. Este modelo se desarrolló a partir de un proyecto de investigación patrocinado por el departamento de defensa de los Estados Unidos denominado ARPANET. Esta red debería permanecer funcionando en caso de que algunos de los nodos de la red o incluso sus conexiones fueran dañados por algún motivo. La red ARPANET empezó conectando centros de investigación del gobierno y luego universidades hasta convertirse en la red más popular de uso público hasta el momento: Internet.

Un modelo que surge de ARPANET y de los desarrollos posteriores fue el modelo de TCP/ IP. Difiere del modelo de referencia OSI en que no maneja siete capas

sino cinco (en el modelo de TCP/ IP no hay capas para sesión y presentación), según muestra la siguiente figura :



3.1 Capa Física

La capa física se encarga del transporte de los bits de un extremo al otro del medio de transmisión. Debe asegurarse de que cuando un extremo envía un “0” el extremo distante reciba efectivamente un “0”.

A nivel de la capa física las recomendaciones y estándares establecen interfaces mecánicas, eléctricas y de procedimiento, teniendo en cuenta las características del medio de transmisión (ancho de banda, ruido o interferencia, características de propagación).

En las redes LAN, el medio de transmisión históricamente utilizado fue el cable coaxial, y ha sido sustituido actualmente por los cables UTP (par trenzado no blindado) y STP (par trenzado blindando), o por fibras ópticas. Las redes inalámbricas están teniendo también amplia difusión, y utilizan el “ether” (el vacío), como medio de transporte.

En las redes WAN, los medios de transmisión varían, desde los pares de cobre hasta las fibras ópticas o las redes inalámbricas.

3.2 Capa de Enlace

La función principal de la capa de enlace es lograr una comunicación eficiente y confiable entre dos extremos de un canal de transmisión. Para ello, la capa de enlace realiza las siguientes funciones:

- **Armado y separación de tramas:** Dado que la capa física solamente acepta y transmite bits, sin preocuparse de su significado o estructura, corresponde a la capa de enlace crear y reconocer los límites de las tramas de datos.
- **Detección de errores:** Corresponde a la capa de enlace resolver los problemas de tramas dañadas, repetidas o perdidas. Por ejemplo, si no se recibe el acuse de recibo de una trama determinada, puede ser por que la trama original se perdió, o porque llegó correctamente pero se perdió el acuse de recibo. La capa de enlace debe ser capaz de resolver éste tipo de casos.
- **Control de flujo:** La capa de enlace debe resolver los problemas que surgen debido a las diferentes velocidades de procesamiento del receptor y emisor. Debe tener algún tipo de regulación de tráfico, para que no existan saturaciones o desbordes de memorias (buffers)
- **Adecuación para acceso al medio:** En TCP/IP la capa de enlace dispone de una “sub-capa” de acceso al medio (MAC Médium Access Control). Esta sub-capa de acceso al medio implementa los protocolos necesarios para utilizar un medio compartido en las redes de difusión. Esta sub-capa debe resolver las “colisiones” (resultantes de que varias máquinas intenten enviar tramas a la vez sobre un mismo medio compartido)

3.3 Capa de Red

La capa de red es la encargada de hacer llegar la información desde el origen hasta el destino. Para esto puede ser necesario pasar por varias máquinas intermedias. Es de hacer notar la diferencia con la capa de enlace, cuya función se limita a transportar en forma segura tramas de un punto a otro de un canal de transmisión.

La capa de red puede brindar servicios “orientados a la conexión” o “no orientados a la conexión”. En los servicios “orientados a la conexión”, la complejidad se encuentra en la propia capa de red. En los servicios “no orientados a la conexión”, la complejidad es pasada una capa más arriba, es decir, a la capa de transporte. En el funcionamiento “orientados a la conexión”, la capa de red establece “circuitos virtuales” en el proceso de conexión. En el funcionamiento “no orientado a la conexión”, los paquetes enviados se llaman normalmente “datagramas”

3.4 Capa de Transporte

La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina de destino, independientemente de la red o redes físicas en uso. Es la primera capa en la que los corresponsales son directamente los extremos. Para lograrlo, la capa de transporte hace uso de los servicios brindados por la capa de red.

De la misma manera que hay dos tipos de servicios de red, orientados y no orientados a la conexión, hay dos tipos de servicios de transporte, orientados y no orientados a la conexión.

La Internet tiene dos protocolos principales a nivel de la capa de transporte:

- **TCP (Transmission Control Protocol):** Es un protocolo orientado a la conexión, que proporciona flujos de información seguros y confiables.
- **UDP (User Datagram Protocol):** Es un protocolo no orientado a la conexión, muy sencillo (básicamente el paquete IP más un encabezado), y no seguro.

3.5 Capa de Aplicación

En la capa de aplicación residen las aplicaciones de los usuarios. Las capas por debajo de la de aplicación existen únicamente para brindar un transporte confiable a las aplicaciones residentes en la capa de aplicación.

En la capa de aplicación se implementan los temas de seguridad, presentación de la información, y cualquier aplicación útil para los usuarios (correo electrónico, world wide web, etc.).

4 Redes LAN

Las redes de área local (LAN: Local Area Network) son aquellas que conectan una red de ordenadores normalmente confinadas en un área geográfica, como un solo edificio o un campus. Las LAN, sin embargo, no son necesariamente simples de planificar, ya que pueden unir muchos centenares de ordenadores y pueden ser usadas por muchos miles de usuarios. El desarrollo de varias normas de protocolos de red y medios físicos, junto con la baja de precio de las computadoras han hecho posible la proliferación de LAN's en todo tipo de organizaciones.

Las LAN generalmente utilizan transmisión por difusión, a velocidades de 10, 100 o 1000 Mb/s. Las topologías más utilizadas son en bus (IEEE 802.3 Ethernet) o en anillo (IEEE 802.5 Token Ring)

4.1 Ethernet

Ethernet fue desarrollada originalmente por Bob Metcalfe, trabajando para Xerox [2]. Le había sido asignada la tarea de desarrollar un mecanismo para interconectar los computadores que en ese momento se estaban desarrollando en la Compañía. Inspirado en los trabajos publicados por la Universidad de Hawaii, respecto a la red “Alohanet” [3], en 1973 Bob Metcalfe desarrolló una nueva tecnología de comunicación entre computadores, a la que llamó “Ethernet”.

Ethernet fue tan exitosa, que en 1980 varias compañías la adoptaron. Digital, Intel y Xerox comenzaron a usarla, a velocidades de 10 Mb/s, convirtiéndola en un “estándar de hecho”.

En febrero de 1980 la Sociedad de Computación del IEEE realizó la primer reunión del “comité de estandarización de redes de área local” (“Local Network Standards Committee”), al que fue asignado el número 802 (simplemente el siguiente número secuencial de los proyectos que estaban en curso en la IEEE). En 1983 Ethernet es estandarizada como IEEE 802.3 (10 Base 5). Desde entonces, varias recomendaciones se han incorporado a la original 802.3. Las principales se detallan a continuación [4].

Recomendación	Año	Descripción
802.3a	1985	10Base2 (thin Ethernet)
802.3c	1986	10 Mb/s repeater specifications (clause 9)
802.3d	1987	FOIRL (fiber link)
802.3i	1990	10Base-T (twisted pair)
802.3j	1993	10Base-F (fiber optic)
802.3u	1995	100Base-T (Fast Ethernet and autonegotiation)
802.3x	1997	Full-duplex
802.3z	1998	1000Base-X (Gigabit Ethernet)
802.3ab	1999	1000Base-T (Gigabit Ethernet over twisted pair)
802.3ac	1998	VLAN tag (frame size extension to 1522 bytes)

802.3ad	2000	Parallel links (link aggregation)
802.3ae	2002	10 Gigabit Ethernet
802.3af	2003	PoE (Power over Ethernet)

Ethernet es la tecnología de LAN más popularmente utilizada actualmente. Ethernet es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría los usuarios de la informática actual. Adhiriéndose a las normas de IEEE, los equipo y protocolos de red pueden interoperar eficazmente.

Un “sistema Ethernet” dispone básicamente de tres elementos:

- El **medio físico,** que transporta las señales entre las máquinas.
- Un conjunto de **reglas de acceso al medio físico**, incluidas en las “Interfaces Ethernet”, que permiten que varias máquinas puedan acceder al mismo medio sin necesidad de arbitrajes externos.
- Una “**trama Ethernet**” que consiste en una secuencia de bits estandarizada.

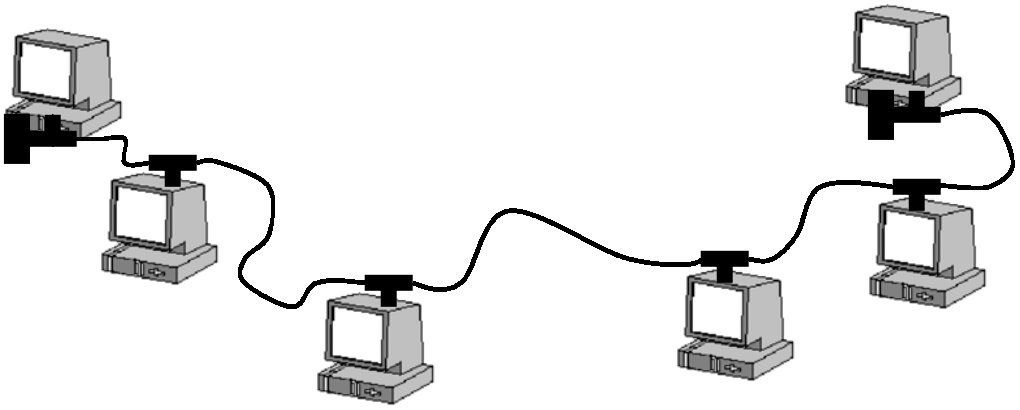
4.1.1 El medio físico en Ethernet

Ethernet admite cuatro tipos de medios físicos cableados:

- Cable Coaxial Grueso ("Thick wire" o "Thick Ethernet") (10BASE5)
- Cable Coaxial Fino ("Thin wire" o "Thin Ethernet") (10BASE2)
- Par Trenzado Sin Malla ("Unshielded Twisted Pair" o "UTP") para redes 10BASE-T, 100BASE-T o 1000BASE-T
- Fibra Optica ("Fiber optic") para redes 10BASE-FL o para redes de Vínculos Inter-repetidores de Fibra Optica ("Fiber-Optic Inter-repeater Link" o "FOIRL").

Esta amplia variedad de medios refleja la evolución de Ethernet y también demuestra la flexibilidad de la tecnología.

Las primeras redes Ethernet funcionaban sobre cables coaxiales que recorrían, formando un “bus”, cada una de las máquinas de la red.



Thickwire fue uno de los primeros sistemas de cableado coaxial utilizados en Ethernet pero era difícil de trabajar y caro. Este evolucionó al cable coaxial fino, el cual es más fácil de trabajar y más barato. Sin embargo, una debilidad de las redes basadas en cables coaxiales fue la poca fiabilidad. Un problema en cualquier punto del cable afectaba a toda la red. Más recientemente, se comenzó a utilizar cable de cobre trenzado sin malla (UTP) y concentradores ("hubs" Ver 4.2).

Hoy, los más populares esquemas de cableado son 10BASE-T y 100BASE-TX los cuales utilizan cable de par trenzado sin malla (UTP). Estos cables se clasifican en "Categorías", de acuerdo al ancho de banda de los mismos. Un estudio detallado de estas Categorías y sus características puede verse en "Cableado Estructurado" [5]

Para aplicaciones especializadas pueden utilizarse fibras ópticas. El cable de fibra óptica es más costoso, pero es insustituible para situaciones donde las emisiones electrónicas y los riesgos ambientales son un problema a tener en cuenta.

El cable de fibra óptica es a menudo utilizado para aplicaciones inter-edificio para aislar equipamientos de red de daños eléctricos ocasionados por descargas de rayos debido a que este no conduce electricidad.

El cable de fibra óptica puede también ser útil en áreas donde hay gran interferencia electromagnética, como por ejemplo el piso de una fábrica.

El estándar Ethernet permite segmentos de cable de fibra óptica de hasta 2 kilómetros de longitud, convirtiendo a la Ethernet por fibra óptica en la elección perfecta para conexión de nodos y edificios que de otro modo no serían alcanzables por medios de conductores de cobre.

Ethernet también admite medios físicos inalámbricos, como se verá en el capítulo 4.5.

4.1.2 Reglas de acceso al medio físico en Ethernet

Cada máquina Ethernet opera en forma independiente del resto de las máquinas de la red. Ethernet no dispone de controladores centrales. Cada máquina en la red

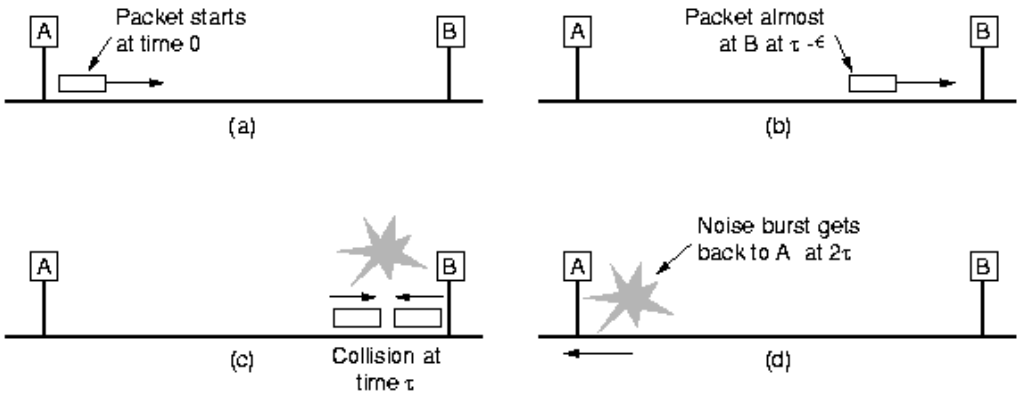
está conectada al mismo medio de transmisión compartido. Las señales Ethernet que genera cada máquina son transmitidas en forma serial, un bit a continuación de otro, sobre el medio físico compartido. Para enviar datos, las máquinas tratan de asegurarse que el medio físico esté “libre” (es decir, que ninguna otra máquina está transmitiendo bits). Para ello “escuchan” el medio físico, y cuando entienden que está libre, transmiten los datos en la forma de una “trama Ethernet”. Luego de la transmisión de cada trama, todas las máquinas de la red compiten nuevamente por el medio para el envío de nuevas tramas. Esto asegura que el acceso al medio físico es equitativo, y que ninguna máquina puede bloquear el acceso de las otras. Las reglas de acceso al medio físico están determinadas por una sub-capa de control de acceso al medio, llamada MAC (Medium access control). Las funciones de esta sub-capa están generalmente incorporadas en las interfaces Ethernet de cada máquina. El mecanismo de control de acceso al medio está basado en un sistema denominado CSMA/CD (Carrier Sense Multiple Access with Collition Detection).

Como se mencionó, las máquinas de una red Ethernet envían paquetes cuando determinan que la red no está en uso. Esta determinación se hace esperando un tiempo (cuya duración es aleatoria) después del último paquete que se está transmitiendo en la red en ese momento. Transcurrido este tiempo, sin detectar actividad en el medio físico, se determina que la red esta disponible para efectuar una transmisión. Sin embargo, es posible que dos máquinas en localizaciones físicas distantes traten de enviar datos al mismo tiempo. Cuando ambas máquinas intentan transmitir un paquete a la red al mismo tiempo se produce una colisión. Este mecanismo puede asimilarse al que utilizamos los humanos al conversar: cada uno espera un tiempo (aleatorio) desde que el otro emitió la última palabra antes de determinar que terminó de decir lo que quería y proceder entonces a contestar. Si por algún motivo erramos en la determinación, hablaremos dos o más al mismo tiempo, generando una “colisión” y deberemos detenernos y re-comenzar.

Minimizar las colisiones es un elemento crucial en el diseño y operación de redes. El incremento de las colisiones es a menudo el resultado de demasiados usuarios en una red, lo que produce una notable disminución en el ancho de banda efectivo de la red. Esto puede enlentecer la performance de la red desde el punto de vista de los usuarios. Segmentar la red en varios “dominios de colisión”, con un "bridge" o un "switch", es una manera de reducir una red superpoblada (Ver 4.3).

El tamaño máximo de una red Ethernet está determinada por el largo mínimo de una trama y la velocidad de la misma, debido a la necesidad de detectar colisiones. Se debe evitar que una máquina complete la transmisión de una trama antes de que el primer bit de dicha trama llegue hasta la máquina más alejada de la red y eventualmente vuelva a la máquina de origen.

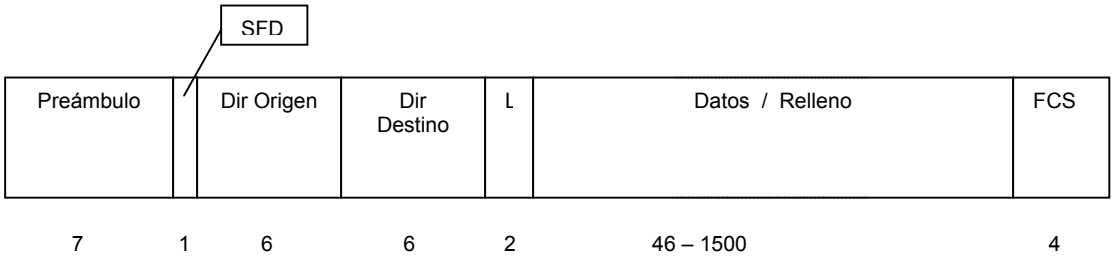
Supongamos que la máquina A comienza a transmitir el primer bit de una trama en el tiempo 0, y que este bit tarda un tiempo ζ en llegar a la máquina más lejana B. Supongamos que casualmente la máquina B decide comenzar el envío de una trama justo antes de ζ, digamos a un tiempo $\zeta - \varepsilon$. Inmediatamente se producirá una colisión, que será detectada sin problemas por la máquina B, pero esta



colisión tardará otro tiempo ζ en llegar hasta la máquina A. Es decir, la máquina A recibirá la información de la colisión a un tiempo 2 ζ desde el comienzo del envío del primer bit de su trama. Si la máquina A hubiera terminado el envío de su trama antes de 2 ζ, no hubiera detectado esta colisión, y por lo tanto, hubiera asumido que la trama fue enviada correctamente.

Dado que las tramas tienen un largo mínimo de 64 bits, conociendo el tiempo de propagación (teniendo en cuenta los posibles repetidores y sus retardos), puede calcularse la distancia máxima de una red Ethernet, según la velocidad de transmisión de bits (en bits/s). Para 10 Mb/s, la distancia máxima es de 2.500 m (previendo 4 repetidores).

4.1.3 Trama Ethernet



La estructura de la trama Ethernet se muestra en la figura. Comienza con 7 bytes de “preámbulo”, que contienen los bits “10101010” como un patrón fijo. Dado que Ethernet utiliza codificación Manchester, este patrón genera una onda cuadrada de 10 Mhz durante 5.6 µs, lo que permite sincronizar los relojes de las máquinas receptoras con el reloj de la máquina que origina la trama.

Luego del preámbulo se transmite el byte “10101011”, indicando el comienzo efectivo de la trama.

La trama misma contiene la información de origen y destino. Las direcciones Ethernet consisten en 6 bytes, los primeros 3 correspondientes al fabricante del

controlador Ethernet (excluyendo los 2 primeros bits, que están reservados), y los últimos 3 al número de dispositivo fabricado.

Con 46 bits, hay aproximadamente 7 x10^{13} direcciones Ethernet posibles.

La dirección consistente en todos los bits en 1 es reservada para “difusión” (broadcast). Una trama que contiene todos los bits en 1 en la dirección de destino es recibida y procesada por todas las máquinas de la red.

El campo “L” indica la longitud del campo de datos, desde 0 a 1500. Dado que las tramas Ethernet deben tener como mínimo 64 bytes, si los datos a transmitir son menos de 46 bytes, se completan con “relleno”.

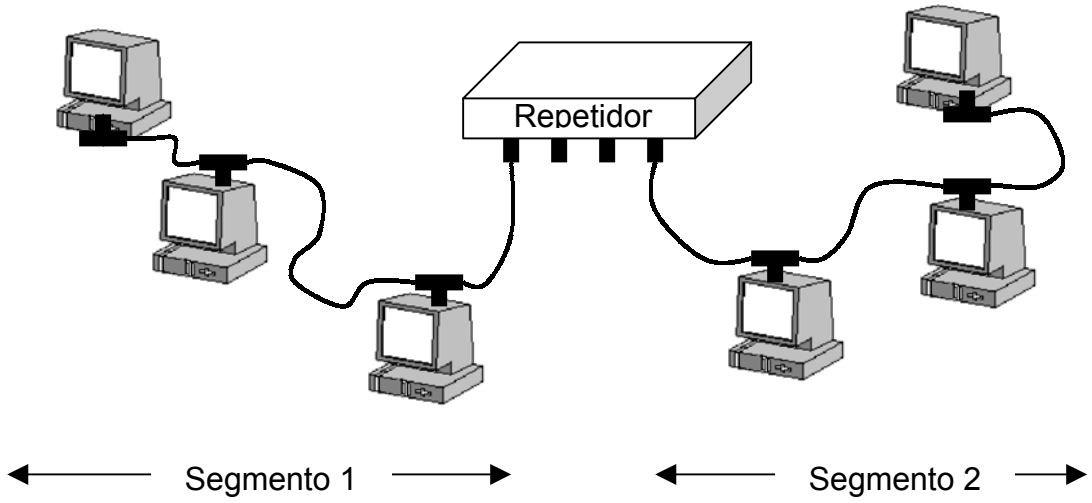
El campo final FCS (Frame Check Sequence) es la “suma de comprobación”, utilizada por el receptor para validar la ausencia de errores en la trama recibida.

4.2 Hubs

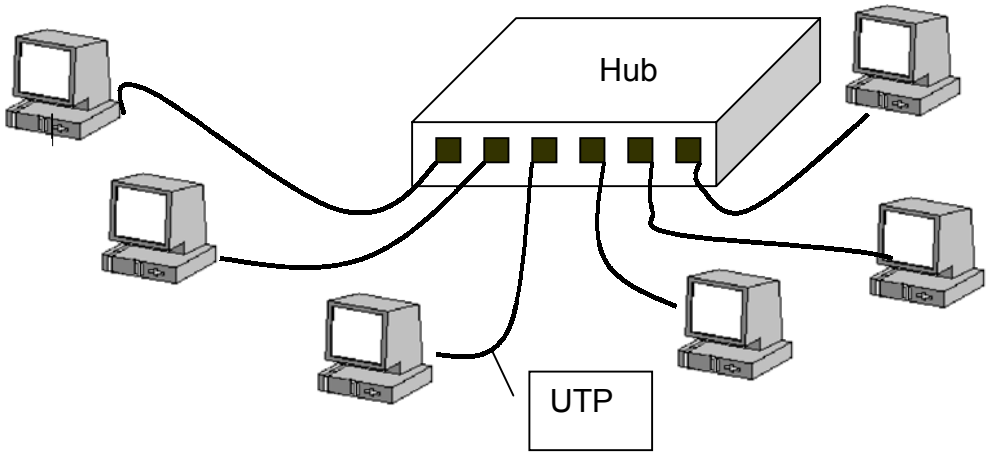
Como se indicó en 4.1.1, las primeras redes Ethernet utilizaron cables coaxiales como medios físicos, y luego evolucionaron a cables UTP (pares de cobre trenzados sin malla).

Debido a los retardos y la atenuación de las señales, fue necesario determinar longitudes máximas y cantidades máximas de máquinas en las redes coaxiales. Para que la red funcione correctamente, un segmento de cable coaxial fino puede tener hasta 185 metros de longitud y hasta 30 nodos o máquinas. Un segmento de cable coaxial grueso puede tener hasta 500 metros, y hasta 100 nodos o máquinas.

Las redes coaxiales grandes requerían ampliar estas restricciones, para lo que se desarrollaron “repetidores”, capaces de conectar varios segmentos de la red. Los repetidores proporcionan la amplificación y resincronización de las señales necesarias para conectar los segmentos entre sí. Al poder conectar varios segmentos, permitimos a la red continuar creciendo, sin violar las restricciones de correcto funcionamiento.



Al utilizar cable UTP, cambió la topología del cableado. Las redes coaxiales utilizaban una topología de bus, dónde el cable coaxial recorría todas las máquinas de su segmento. Las redes UTP son siempre en estrella, por lo que es siempre necesario un concentrador que a su vez realice las funciones de repetidor. Este equipo se conoce habitualmente como “Hub”



En las redes Ethernet sobre UTP se disponen siempre de un enlace “punto a punto”, desde la máquina o PC hasta un Hub, formando por lo tanto una topología en estrella, con el Hub en el centro de la misma.

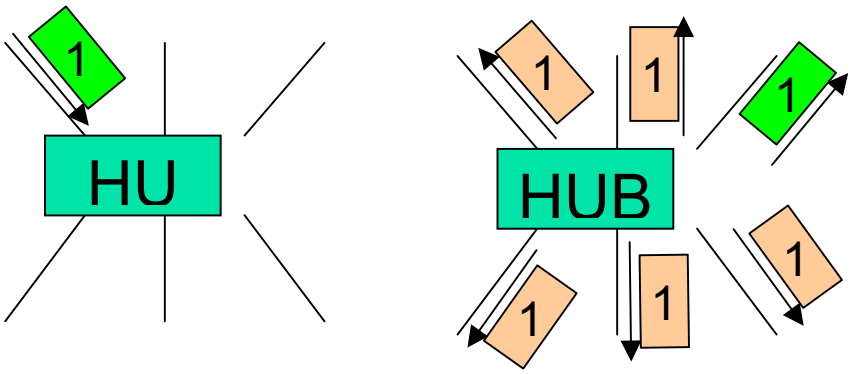
La función principal del Hub es la de repetir la señal que ingresa por cada una de sus “puertas” hacia todas las otras “puertas”, realizando por tanto la “difusión” que requiere Ethernet (y que se daba naturalmente en las topologías de bus sobre cables coaxiales).

Adicionalmente, los Hubs también monitorizan el estado de los enlaces de las conexiones a sus puertas, para verificar que la red funciona correctamente (una

puerta de un Hub puede tener conectada una máquina o un segmento proveniente de otro Hub). En las redes coaxiales, cuando algo falla en un determinado segmento (por ejemplo se produce una rotura en un cable o en un conector), todas las máquinas conectadas a ese segmento pueden quedar inoperantes. Los Hubs limitan el efecto de estos problemas, desconectando el puerto problemático y permitiendo al resto seguir funcionando correctamente. La avería de un cable o conector en una red punto a punto, habitualmente, sólo desactivará una máquina, lo que en una topología de bus ocasionaría la desactivación de todos los nodos del segmento.

Las recomendaciones IEEE 802.3 describen las reglas para el número máximo de repetidores (Hubs) que pueden ser usados en una configuración. El número máximo de repetidores (Hubs) que pueden encontrarse en el camino de transmisión entre dos máquinas es de cuatro; el máximo número de segmentos de red entre dos máquinas es cinco, con la restricción adicional de que no más de tres de esos cinco segmentos pueden tener otras estaciones de red conectadas a ellos (los otros segmentos deben de ser enlaces entre repetidores, que simplemente conectan repetidores). Estas reglas son determinadas por cálculos de las máximas longitudes de cables y retardos de repetidores. Las redes que las incumplen puede que aún funcionen, pero están sujetas a fallos esporádicos o problemas frecuentes de naturaleza indeterminada. Además, usando repetidores, simplemente extendemos la red a un tamaño mayor. Cuando esto ocurre, el ancho de banda de la red puede resultar un problema; en este caso, los “switches” (conmutadores) pueden usarse para particionar una gran red en segmentos más pequeños que operan más eficazmente (Ver 4.3).

Lo más importante a resaltar sobre los Hubs es que sólo permiten a los usuarios compartir Ethernet, es decir, implementar un medio físico. Una red que utiliza Hubs es denominada "Ethernet compartida", lo que implica que todos los miembros de la red compiten por el uso del medio, formando por lo tanto un único “dominio de colisión”. Cuando una máquina debe enviar una trama de datos a otra,



la misma es recibida por el Hub en una de sus puertas, y retransmitida a todas las otras puertas. Los Hubs no interpretan el contenido de las tramas. Trabajan a nivel eléctrico (físico), regenerando las señales y retransmitiéndolas.

4.3 Bridges

La función de los “Bridges” (“puentes”) es interconectar redes de distintas tecnologías. Los bridges pueden conectar entre si tipos de redes diferentes (como por ejemplo Ethernet con Fast Ethernet, Ethernet con Token Ring, etc.). Para ello, deben interpretar la trama que reciben por una de sus “puertas” y “traducirla” al formato adecuado de la puerta de salida. Por lo tanto, los Bridges debe trabajar a nivel de la “Capa 2” o Capa de Enlace.

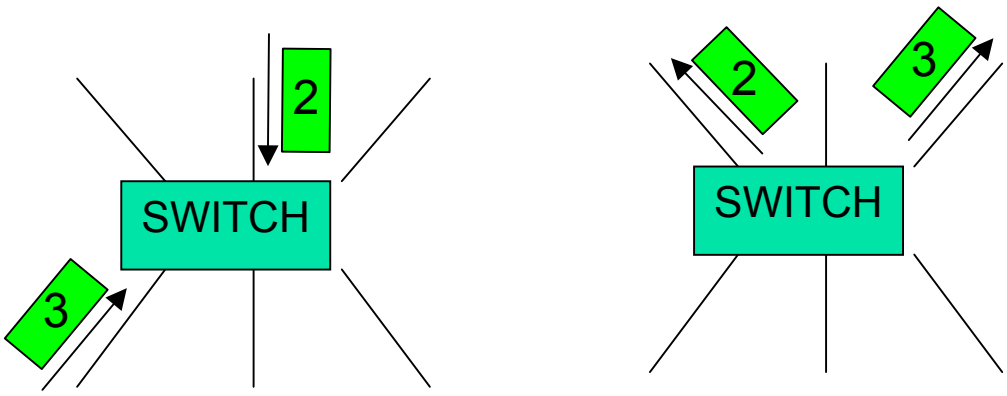
4.4 Switches

4.4.1 Introducción a los Switches

Como se mencionó en 4.2, los Hubs son concentradores y repetidores, que trabajan a nivel de la capa física, regenerando la señal que reciben por una de sus puertas y retransmitiéndola por todas las otras puertas.

Sin embargo, cuando las redes comienzan a crecer, la probabilidad de colisiones también crece, generando más retransmisiones, y por lo tanto degradando la performance general de la red. Para solucionar, o por lo menos disminuir este problema, pueden utilizarse “Switches” o “Conmutadores”.

Los “Switches” son dispositivos que analizan las tramas Ethernet, y la envían a la puerta adecuada de acuerdo a la dirección de destino. A diferencia de los Hubs, que trabajan a nivel de la “Capa 1” (capa física), los switches trabajan a nivel de la “Capa 2” (capa de enlace).



Esto permite que varias máquinas puedan estar enviando tramas a la vez, y no existan colisiones.

Para que esto sea posible, los switches deben conocer las direcciones de enlace (conocidas como “direcciones MAC” en Ethernet) conectadas a cada uno de sus puertos. La mayoría de los switches “aprenden” de manera automática las direcciones MAC conectadas a cada puerto en forma automática. Simplemente,

cuando reciben una trama por una puerta, obtienen la dirección de origen y la asocian a la puerta por la que se recibió la trama. Si por una puerta reciben una trama dirigida a una dirección MAC destino desconocida, envían la trama por todos los puertos (como lo haría un Hub). Cuando la máquina de destino responda, el switch "aprenderá" en que puerta se encuentra su dirección y las próximas tramas serán enviadas únicamente a esa puerta.

Dado que una puerta de un switch puede estar conectado a otro switch o hub, es posible que una misma puerta esté asociada a un conjunto de direcciones MAC. Los switches habitualmente pueden almacenar varios cientos o miles de direcciones MAC por puerta.

Los paquetes del tipo "Broadcast" son enviados a todas las puertas del switch.

Los switches tienen básicamente dos mecanismos de funcionamiento: "store and forward" (almacenar y remitir) y "cut through" (cortar y atravesar):

- **"Store and Forward":** Esta mecanismo de trabajo consiste en recibir por una puerta una trama completa, para luego analizarla y retransmitirla.
- **"Cut through":** Dado que la dirección de destino se encuentra al comienzo de la trama (ver 4.1.3), este modo de trabajo consiste en analizar únicamente los primeros bytes de la trama, hasta obtener la dirección de destino, e inmediatamente comenzar a retransmitir la trama.

El método "Cut through" parece a priori más rápido, ya que no espera la recepción completa de la trama para luego retransmitirla. Sin embargo, este método no puede validar que la trama recibida sea correcta (ya que comienza a enviarla antes de recibirla en su totalidad). Si la trama recibida tuviera errores (o existieran colisiones en el segmento de red conectado a la puerta del switch por el que ingresa la trama), éstos errores se propagarán a la puerta de salida del switch. Por el contrario, el método "Store and Forward" puede detectar los errores o colisiones en las tramas de entrada, y descartarlas antes de enviarlas a la puerta de salida. Muchos switches pueden trabajar con ambos métodos, y el administrador de red puede decidir cual es el mejor en cada caso.

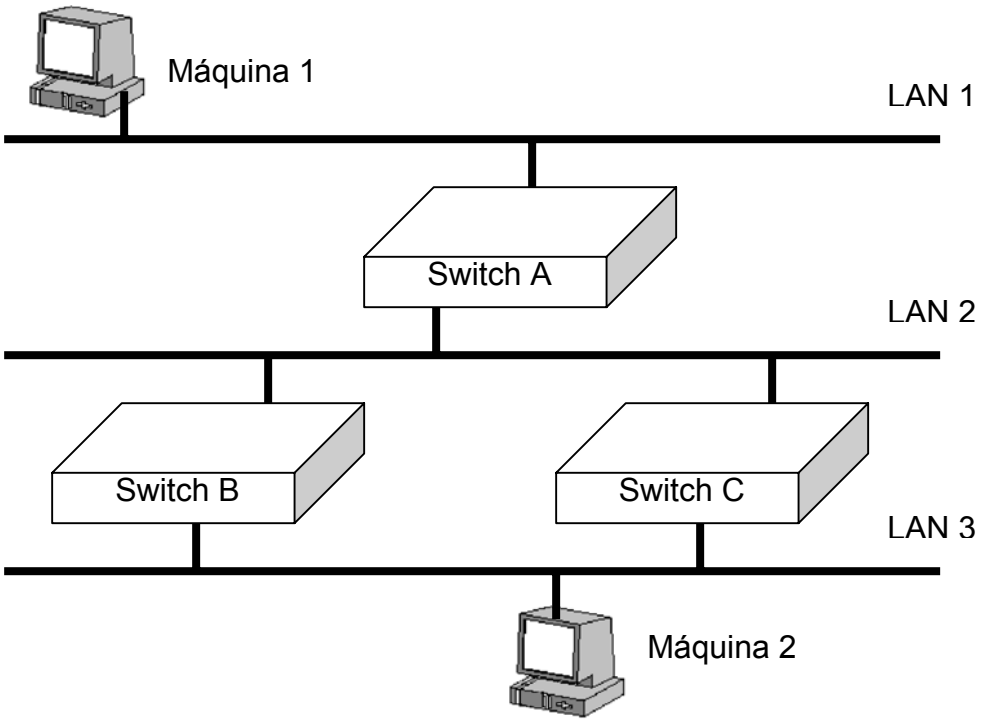
Muchos de los "switches" disponibles en el mercado tienen, en el mismo equipo, puertas Ethernet, Fast Ethernet y/o Gigabit Ethernet, sobre UTP o sobre Fibra óptica, por lo que realizan implícitamente funciones de Bridges (o puentes).

4.4.2 Spanning Tree

Un potencial problema que se presenta al implementar una red con Hubs y Switches es la posibilidad de crear bucles o "loops" entre ellos. Pongamos por ejemplo una red como la que se muestra en la figura y veamos como se comporta:

1. Supongamos que luego del encendido inicial de los swtiches A, B y C, la Máquina 1 envía una trama dirigida a la máquina 2
2. El Switch A recibe la trama y registra la dirección de origen (dirección MAC de la Máquina 1) en su tabla de direcciones, asociándola al puerto

correspondiente (el superior en la figura). Luego analiza la dirección MAC de destino, y al no encontrarla en sus tablas (se supone que el switch acaba de ser inicializado) difunde las tramas por todas sus puertas, y en particular, hacia la LAN 2



3. En la LAN 2, la trama es recibida por el Switch B y por el Switch C. Ambos switches registran la dirección MAC de la máquina 1 en sus puertas superiores, comparan la dirección de destino con sus tablas, y al no encontrarla, difunden la trama por todas sus puertas, y en particular por las puertas conectadas a la LAN 3. Esto resulta en que dos tramas idénticas son enviadas a la LAN 3.
4. La trama enviada a la LAN 3 por el switch B es recibida por la Máquina 2, pero también por el Switch C. El Switch C al recibir la trama, inspecciona la dirección de origen, y encuentra que la tenía asignada a la puerta superior. Entiende que la Máquina 1 cambió de lugar, y actualiza sus tablas, asociando la dirección de la Máquina 1 al puerto inferior (LAN 3). Por otra parte, la dirección de destino de la trama, correspondiente a la Máquina 2 aún es desconocida por el Switch C, por lo que envía la trama nuevamente a la LAN 2.
5. Si el Switch B es más lento que el Switch C, puede recibir la trama nuevamente por su puerta superior (LAN 2) y reenviarla nuevamente a la LAN 3, quedando por tanto la trama en “bucle”.

6. Si el Switch B realizó el mismo proceso que el Switch C antes de recibir la trama por la LAN 2, habrá asociado, al igual que el Switch B, la dirección de la Máquina 1 como perteneciente a la LAN 3. Cuando la Máquina 2 responda, ambos switches entenderán que la dirección de la Máquina 1 corresponde a la LAN 3 y descartarán la trama.

Como se explicó, si existen bucles en la interconexión de switches, una trama puede quedar "atrapada" eternamente en un bucle, degradando completamente la performance de la red, o pueden descartarse tramas, imposibilitando la comunicación. Para evitar esta situación, se ha desarrollado un algoritmo conocido como "Spanning Tree", que se ha estandarizado en la Recomendación IEEE 802.1d [6]. La idea de este algoritmo es bloquear los enlaces que cierran los bucles, dejando a la red siempre con una topología del tipo "árbol", y asegurar de esta manera que no existan bucles.

El algoritmo reevalúa periódicamente que enlaces hay que bloquear o rehabilitar para tener acceso a todos los equipos sin crear bucles. Por ello, utilizando adecuadamente el algoritmo "Spanning Tree" es posible armar explícitamente configuraciones en bucle que permitan tener enlaces de respaldo en caso de falla en los enlaces principales. Dado que el algoritmo permite valorar los enlaces con "pesos", cuando existen bucles es posible configurar a priori que enlaces serán los principales y que enlaces quedarán bloqueados.

4.4.3 VLANs

Como se mencionó en 4.4, los switches mejoran la performance de las redes enviando las tramas únicamente a las puertas dónde se encuentra el destino de la misma. Sin embargo, los mensajes de difusión (broadcast) son enviadas a todas las puertas, ya que deben ser recibidos por todas las máquinas de la misma red. A veces es deseable limitar el alcance de los mensajes de difusión (broadcast), y por lo tanto, "la red".

Las "VLANs" (Virtual LANs, o redes LAN virtuales) permiten utilizar los mismos medios físicos para formar varias redes independientes, a nivel de la capa 2. Un mismo conjunto de switches pueden implementar, utilizando VLANs, varias redes LAN independientes.

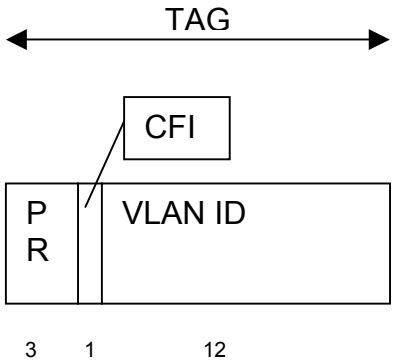
Los criterios para formar las VLAN pueden ser varios. Entre los más comunes se encuentran:

- **VLAN por puertos:** Los puertos de los switches se agrupan en VLANs. De esta manera, las máquinas conectadas a un puerto únicamente "ven" a las máquinas que están conectadas a puertos de la misma VLAN
- **VLAN por direcciones MAC:** Las direcciones MAC se agrupan en VLAN. De esta manera, se pude restringir la red únicamente a ciertas direcciones MAC, independientemente de en que puerto de los switches se conecten.
- **VLAN por protocolo:** Algunos switches que soportan VLAN pueden inspeccionar datos de la capa 3, como el protocolo utilizado, y formar redes independientes según estos protocolos

- **VLAN por direcciones IP:** Las direcciones IP (de capa 3) pueden ser leídas por los switches, y pueden formarse redes independientes con ciertos conjuntos de direcciones IP

Cuando se dispone de un único switch, la implementación de las VLANs es sencilla, ya que todas las reglas se manejan dentro del mismo switch. Sin embargo, ¿qué sucede si una máquina de una VLAN debe comunicarse con otra máquina de la misma VLAN, pero conectada a otro switch? La información de la VLAN de origen, debe "viajar" , junto con la trama, hasta el otro switch. Para esto, se ha estandarizado la recomendación IEEE 802.1q [7], que permite transmitir en las tramas Ethernet la información de VLAN. Conceptualmente es simple: se agregan a la trama Ethernet 4 bytes. La figura muestra una trama Ethernet "normal" y una trama Ethernet 802.1q:

Como puede observarse, se agregan 4 bytes: los primeros 2, llamados "TPI", son fijos e identifican a la trama como una trama 802.1q. Los segundos 2 bytes, llamados "TAG" se interpretan como 3 conjuntos de bits, de longitud 3 bits, 1 bit y 12 bits respectivamente:



Los primeros 3 bits del “TAG” indican la “prioridad” de la trama, de acuerdo a la recomendación IEEE 802.1p [8] (es de hacer notar que el cabezal de 802.1q contiene la marca de priorización 802.1p, por lo que es necesario disponer de 802.1q para interpretar 802.1p).

El cuarto bit, llamado CFI (Canonical Format Indicator), indica el orden de los bits (en formato canónico o no canónico).

Los últimos 12 bits indican la VLAN a la cual pertenece la trama. Estos 12 bits permiten tener, por lo tanto hasta 4096 VLANs

De esta manera, las tramas intercambiadas entre switches pueden contener información de VLAN.

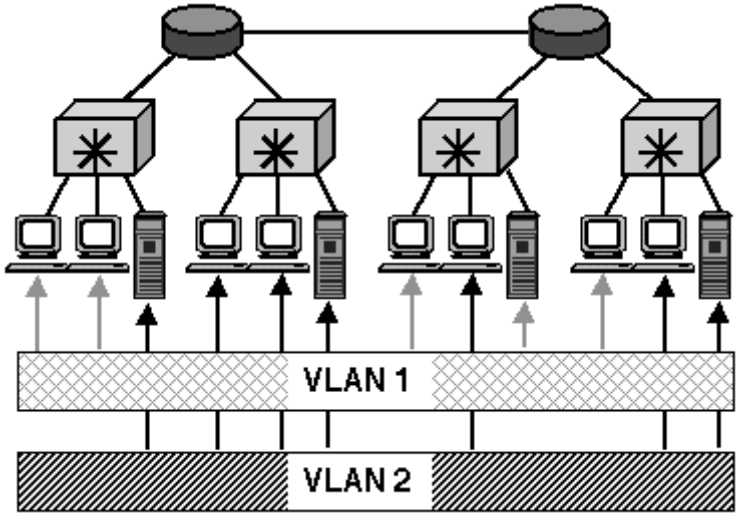
4.4.4 Routing Switches (Switches de capa 3)

Los switches, como se vio anteriormente, son esencialmente bridges multipuerto que aprenden automáticamente que direcciones MAC tienen conectadas a cada puerta. Las tramas que ingresan a un switch, en vez de ser propagadas a todas sus puertas, son enviadas únicamente a la puerta dónde se encuentra la dirección de destino de la trama de entrada.

Los switches mejoran la eficiencia de la red, ya que pueden soportar transmisiones simultáneas, siempre que no involucren las mismas puertas. Sin embargo, los mensajes de difusión (broadcast) son enviados por los switches a todas sus puertas, de la misma manera que las tramas que tienen dirección MAC de destino desconocida. En la mayoría de los casos, el número de máquinas conectadas a una red switcheada puede ser mayor al número de máquinas conectadas a una red “no switcheada” (consistente en hubs), pero los “dominios de broadcast”, aún con switches, continúan siendo una restricción a la cantidad de máquinas de una LAN. Para solucionar este problema, se desarrollaron las VLANs, que separan totalmente los “dominios de broadcast”. Las máquinas pueden ser asignadas a una VLAN de acuerdo al puerto físico del switch a la que está conectada, de acuerdo al protocolo de capa 3, de acuerdo a su dirección MAC o dirección IP, etc. Las VLAN por direcciones MAC facilitan los problemas de “mudanzas”, mientras que las VLAN por protocolo limitan el impacto de los broadcast generados por ciertos protocolos.

Sin embargo, las VLAN limitan los dominios de broadcast separando completamente las redes. En muchos casos, si bien es deseable limitar los broadcast, también es deseable poder mantener comunicaciones entre máquinas de distintas VLANs. La solución a este problema es utilizar equipos "ruteadores", que analicen más allá de la capa 2 (llegando a la capa 3 o capa de red), y en base a tablas de "ruteo", puedan enviar tráfico entre diferentes VLANs.

Realizar esta tarea con ruteadores "clásicos" (Ver 5.3) es lento a nivel de



performance y costoso económicamente. Por esta razón se han desarrollado los equipos llamados "Routing Switches", o "Switches de capa 3".

Tradicionalmente, el proceso de "ruteo" (a nivel de las direcciones de capa 3, por ejemplo, direcciones IP), es realizado por software, corriendo en uno o varios procesadores relativamente lentos, incluidos en los ruteadores (routers) tradicionales. En contraste, los routing switches pueden realizar ruteo IP (o IPX en algunos casos) en hardware especializado, y a la "velocidad del cable", es decir, a la misma velocidad entrada de los datos (10, 100, 1000 Mb/s).

En suma, los routing switches son equipos que permiten "switchear" (analizar a nivel de capa 2) o rutear (analizar a nivel de capa 3) las tramas y paquetes que reciben. Permiten por tanto, separar dominios de broadcast y a su vez permitir comunicaciones entre máquinas de distintos dominios. Su administración se asemeja a la de un router tradicional (Ver 5.3), pero con la ventaja de ser sumamente rápido (a la "velocidad del cable").

4.5 Redes inalámbricas (Wireless LAN)

Cuando es necesario disponer de movilidad en las comunicaciones, depender de un enlace físico como es un cable (en cualquiera de sus modalidades) supone una seria restricción. Para evitar esto, las conexiones inalámbricas se convierten en una buena alternativa.

Desde hace algunos años, el potencial de esta clase de redes hizo que aparecieran los primeros sistemas que utilizaban ondas de radio para interconectar ordenadores. Estos primeros sistemas inalámbricos eran dependientes totalmente de su fabricante en cuanto a implantación y conectividad, lentos (con velocidades de 1,5 Mb/s) y concebidos para cubrir un reducido grupo de aplicaciones. Pero con el desarrollo tecnológico alcanzado en el transcurso de estos últimos años, han ido apareciendo nuevas soluciones ampliamente estandarizadas y funcionales, en la que se pueden comunicar sistemas informáticos y dispositivos de diversa naturaleza y capacidades mediante la tecnología inalámbrica basados en la emisión de ondas de radio o de luz infrarroja.

Surge entonces el concepto de WLAN (Wireless Local Area Network) que se corresponde con un sistema de comunicación de datos inalámbrica utilizado como alternativa o extensión de la redes locales cableadas.

Este tipo de redes se diferencia de las convencionales principalmente en la capa física y en la capa de enlace de datos, según el modelo de referencia OSI. La capa Física (PHY) indica cómo son enviados los bits de una estación a otra. La capa de Enlace de Datos (MAC) se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores.

En 1997 la IEEE publicó el primer estándar para redes de datos inalámbricas, la Recomendación IEEE 802.11 [9]. Esta recomendación define la sub-capa MAC y la capa física (PHY) para las redes inalámbricas. Desde su publicación inicial, varios grupos de trabajo la han ampliado, en las recomendaciones 802.11a, 802.11b, etc.

La recomendación 802.11a [10] estandariza la operación de las WLAN en la banda de los 5 GHz, con velocidades de datos de hasta 54 Mb/s.

La recomendación 802.11b [11], también conocida con “WiFi”, estandariza la operación de las WLAN en la bada de los 2.4 GHz, con velocidades de datos de hasta 11 Mb/s. Esta recomendación ha sido particularmente exitosa, y existen en el mercado diversos productos que la cumplen.

La recomendación 802.11g [12], estandariza la operación de las WLAN con velocidades de datos de hasta 54 Mb/s. Utiliza la misma banda de 2.4 GHz que la 802.11b, lo que permite que los dispositivos puedan operar en ambas normas. 802.11g utiliza OFDM (orthogonal frequency division multiplexing)

4.5.1 Arquitectura de 802.11

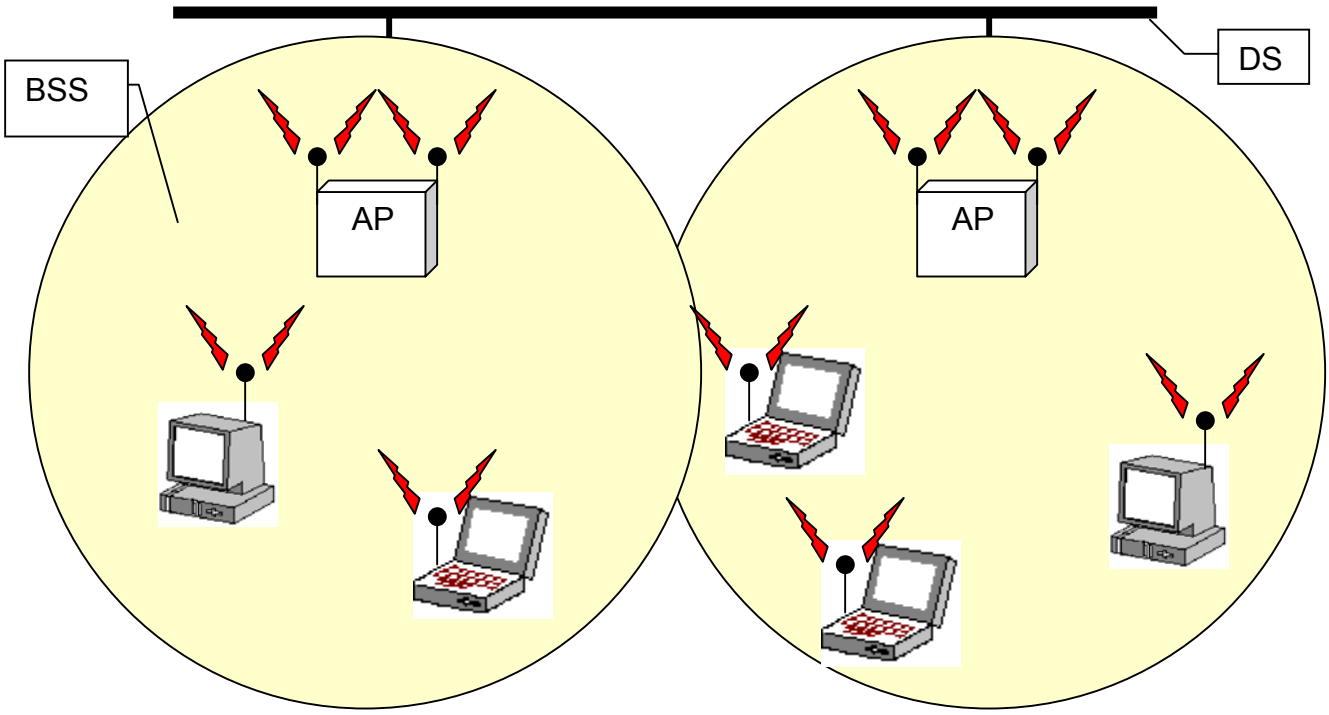
Las redes 802.11 (WLAN) están basadas en una arquitectura del tipo celular, dónde el sistema se subdivide en celdas o células. Cada celda (llamada BSS = Basic Service Set) es controlada por una estación base o punto de acceso (AP = Access Point).

Una WLAN puede estar formada por una única celda, conteniendo un único punto de acceso AP (y como veremos más adelante podría funcionar incluso sin ningún AP), o por un conjunto de celdas cada una con su punto de acceso, los que a su vez se interconectan entre sí a través de un “backbone”, llamado “sistema de

distribución (DS = Distribution System). Este backbone es típicamente Ethernet, generalmente cableado, pero en algunos casos puede ser también inalámbrico.

La WLAN completa (incluyendo las diferentes celdas, sus respectivos AP y el DS) es vista como una única red 802 hacia las capas superiores del modelo OSI.

La siguiente figura ilustra una red 802.11 típica, incluyendo los elementos descritos anteriormente.



La recomendación 802.11 admite dos modos de operación

- "**Infraestructure Mode**": Consiste en disponer por lo menos de un AP (punto de acceso) conectado al DS (Sistema de Distribución)
- "**Ad Hoc Mode**": Las máquinas se comunican directamente entre sí, sin disponer de AP (puntos de acceso) en la red. Dado que no hay AP, todas las máquinas de una red en este modo de operación deben estar dentro del rango de alcance de todas las otras.

4.5.2 Capa física de 802.11

La recomendación 802.11 original fue especificada para trabajar a 1 y 2 Mb/s, en la banda de los 2.4 GHz. Utiliza las técnicas FHSS (Frequency Hopping Spread Spectrum) o DSSS (Direct Sequence Spread Spectrum).

La recomendación 802.11b es una extensión de la recomendación original y trabaja, además de a 1 y 2 Mb/s, también a 5.5 y 11 Mb/s.

Para ello utiliza CCK (Complementary Code Keying) con modulación QPSK (Quadrature Phase Shift Keying) y tecnología DSSS (Direct-Sequence Spread Spectrum).

La recomendación 802.11b soporta cambios de velocidad dinámicos, para poder ajustarse automáticamente a condiciones ruidosas. Esto significa que los dispositivos de una WLAN 802.11b ajustarán automáticamente sus velocidades a 11, 5.5, 2 o 1 Mb/s de acuerdo a las condiciones de ruido.

La recomendación 802.11a es una extensión de la anterior, y trabaja hasta 54 Mb/s en la banda de los 5 GHz. Utiliza técnicas de multiplexación ortogonal por división de frecuencia, en vez de FHSS o DSSS.

4.5.3 Capa MAC de 802.11

El mecanismo de control de acceso al medio está basado en un sistema denominado CSMA/CA (Carrier Sense Multiple Access with Collition Avoidance).

Los protocolos CSMA son los mismos utilizados en Ethernet cableado (Ver 4.1.2). Sin embargo, en Ethernet cableado, se utilizaba el mecanismo de control de acceso CSMA/CD (CSMA con detección de colisiones). En las redes inalámbricas es muy dificultoso utilizar mecanismos de detección de colisiones, ya que requeriría la implementación de equipos de radio “full-duplex” (los que serían muy costosos) y adicionalmente, en las redes inalámbricas no es posible asumir que todas las estaciones puedan efectivamente escuchar a todas las otras (lo que está básicamente asumido en los mecanismos del tipo “detección de colisiones”).

En las redes inalámbricas, el hecho de “escuchar” el medio y verlo “libre” no asegura que realmente lo esté en puntos cercanos. Es por ello que el mecanismo utilizado en las WLAN se basa en evitar las colisiones, y no en detectarlas.

Esto se logra de la siguiente manera:

1. Si una máquina desea transmitir, antes de hacerlo “escucha” el medio. Si lo encuentra ocupado, lo intenta más tarde. Si lo encuentra libre durante un tiempo (denominado DIFS = Distributed Inter Frame Space), la máquina puede comenzar a transmitir.
2. La máquina destino recibe la trama, realiza el chequeo de CRC y envía una trama de reconocimiento (ACK)
3. La recepción de la trama ACK indica a la máquina original que no existieron colisiones. Si no se recibe el ACK, se retransmite la trama hasta que se reciba el ACK, o se supere el máximo número de retransmisiones.

A los efectos de reducir la probabilidad de que dos máquinas transmitan al mismo tiempo debido a que no se escuchan entre sí, la recomendación define un mecanismo de “detección virtual de portadora” (Virtual Carrier Sense), que funciona de la siguiente forma:

Una máquina que desea transmitir una trama, envía primero una pequeña trama de control llamada “RTS” (Request To Send, o “Solicitud para poder Enviar”), que incluye la dirección de origen y destino, y la duración de la siguiente trama

(incluyendo la trama a enviar y su correspondiente respuesta ACK). La máquina de destino responde (si el medio está libre) con una trama de control llamada "CTS" (Clear To Send, o "Todo está libre para que envíes"), que incluye la misma información de duración.

Todas las máquinas reciben el RTS y/o el CTS, y por lo tanto, reciben la información de por cuanto tiempo estará ocupado el medio. De esta manera, tienen un "indicador virtual" de ocupación del medio, que les informa cuánto tiempo deben esperar para poder intentar transmitir.

Este mecanismo reduce la probabilidad de colisiones en el área del receptor. Si existen máquinas que están fuera del alcance del emisor, pero dentro del alcance del receptor, recibirán la trama CTS (enviada por el receptor) y aunque no puedan escuchar la trama del emisor, no ocuparán el medio mientras ésta dure.

4.5.4 Seguridad en redes inalámbricas

Los aspectos de seguridad son especialmente importantes en redes inalámbricas. El comité 802.11 de la IEEE ha abordado el tema, y recomendado el uso del mecanismo de seguridad conocido como "**WEP**" (Wired Equivalent Privacy). Este mecanismo fue diseñado de manera de ofrecer una seguridad equivalente a la que existe en las redes cableadas.

WEP es un algoritmo que encripta las tramas 802.11 antes de ser transmitidas, utilizando RC4. Los receptores desencriptan las tramas al recibirlas, utilizando el mismo algoritmo. Como parte del proceso de encriptación, WEP requiere de una clave compartida entre todas las máquinas de la WLAN, la que es concatenada con una "vector de inicialización" que se genera en forma aleatoria con el envío de cada trama. En suma, WEP utiliza claves de 64 bits para encriptar y desencriptar. Para mejora la seguridad, se desarrolló WEP2, que utiliza claves de 128 bits.

5 Redes WAN

Las redes de área extendida (WAN: Wide Area Network) son aquellas que conectan dos o más redes LAN ubicadas en sitios geográficos distantes.

Las WAN generalmente utilizan protocolos punto a punto, de velocidades bajas a medias (usualmente menores a 2 Mb/s), y se basan en servicios públicos o en líneas punto a punto.

Dadas las características propias de las redes WAN, los protocolos y equipos utilizados difieren de los de las redes LAN.

5.1 Frame Relay

Frame Relay es una tecnología de comunicación utilizada a nivel mundial para interconectar redes LAN, redes SNA, redes de voz, etc. Típicamente se basa en la utilización de la infraestructura de red disponible por los prestadores de servicio público, aunque puede ser también implementada sobre líneas dedicadas.

Frame Relay surgió como es el sucesor de la tecnología X.25, y está pensada para capas físicas con bajas tasas de errores y velocidades relativamente altas (de hasta 2 Mb/s, aunque podría funcionar sin problemas a velocidades mayores).

La tecnología Frame Relay se basa en la utilización de circuitos virtuales (VC = Virtual Circuits) entre las dos redes que se desean conectar. Los circuitos virtuales son caminos bidireccionales, establecidos entre dos puntos extremos de la red Frame Relay. Existen dos tipos de circuitos virtuales:

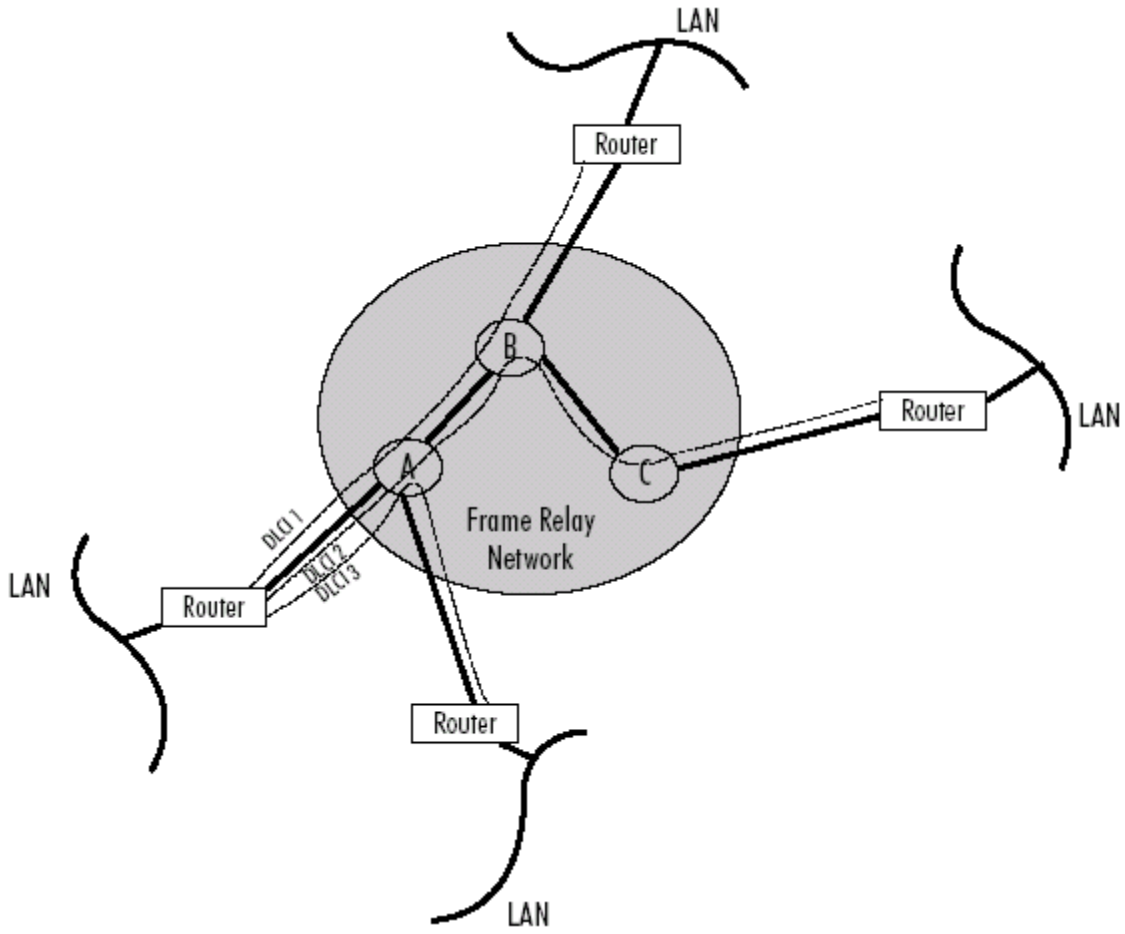
- **PVC (Circuitos virtuales permanentes):** Los PVC son circuitos virtuales permanentes, establecidos por el operador de red (típicamente un prestador de servicios públicos), a través de su sistema de gestión de la red Frame Relay. Los PVC son definidos en forma estática, y se requiere la intervención de un operador para establecerlos y liberarlos. Son “virtuales” ya que puede no existir una conexión física directa entre ambos extremos, sino que por software se pueden configurar todos los equipos intermedios para establecer un “circuito virtual”. Son “permanentes” ya que una vez establecido el circuito, el mismo permanece en el tiempo, en forma independiente del tráfico.

  Los PVC son los más comúnmente utilizados en Frame Relay.

- **SVC (Circuitos virtuales conmutados):** Son circuitos que se establecen en forma dinámica, “llamada a llamada” (en forma similar a una llamada telefónica). La implementación de circuitos virtuales es más compleja que la de circuitos permanentes, pero permite, en principio, conectar cualquier nodo de la red Frame Relay con cualquier otro.

En la siguiente figura se muestra una red Frame Relay típica, dónde 4 nodos (redes LAN) están conectados a una red Frame Relay. Cada nodo dispone de un equipo ruteador (Router), que interconecta la LAN a la red Frame Relay.

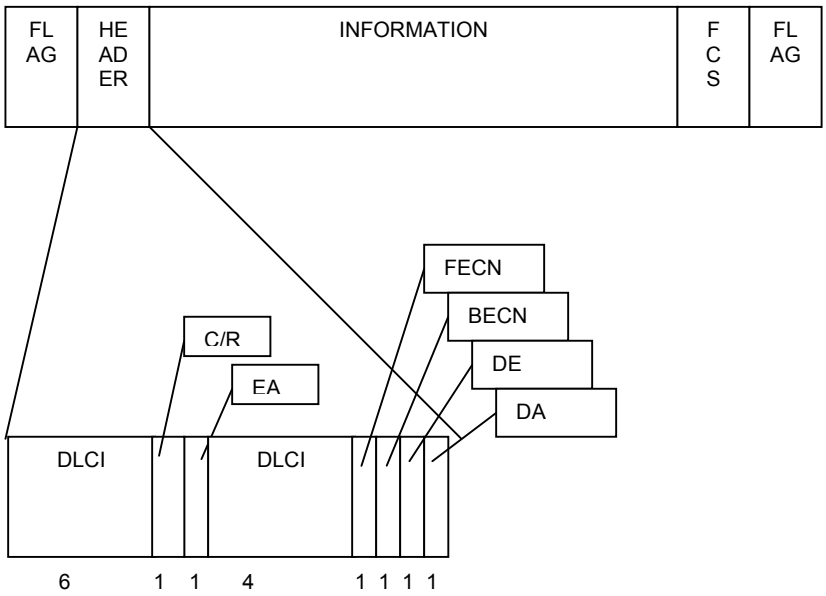
En esta figura, se muestras 3 PVCs establecidos, en forma de estrella. Un extremo de todos los PVC es uno de los nodos de la red, y los otros extremos se encuentran en cada uno de los nodos restantes.



Es de hacer notar que el nodo que recibe los 3 PVCs dispone de un único enlace físico con la red Frame Relay, y no de tres enlaces, como hubiera sido requerido si se utilizara X.25 u otros protocolos punto a punto. Por otro lado, puede verse en la figura, dentro de la red Frame Relay, 3 equipos (A, B, C), administrados por el proveedor del servicio, y configurados para mantener en forma permanente los PVCs.

Desde el punto de vista del modelo OSI, Frame Relay trabaja a nivel de la capa 2, implementado únicamente los aspectos esenciales de la recomendación, como ser chequear que las tramas sean válidas y no contengan errores, pero no solicitando retransmisiones en caso de detectar errores. Frame Relay se basa en la alta confiabilidad de la capa física sobre la que trabaja, y deja a los protocolos de mayor nivel el chequeo de paquetes faltantes, y otros controles de errores.

5.1.1 Trama Frame Relay



La estructura de la trama Frame Relay se indica en la figura. Comienza con un indicador de comienzo de trama (Flag) y una cabecera ("Header") de 2 bytes. Los datos a transmitir (provenientes de capas superiores, como ser paquetes IP, SNA, etc.) se "encapsulan" en la trama Frame Relay, en el campo "Information", luego de la cabecera.

Dentro de la cabecera de la trama se encuentran los siguientes campos:

- **DLCI (Data Link Connection Identifier):** Es un identificador de 10 bits, que indica la dirección de destino de la trama.
- **C/R (Command/Response Field)**
- **FECN (Forward Explicit Congestion Notification):** Cuando la red Frame Relay está congestionada, algunos paquetes pueden ser descartados. Si un nodo dentro de la red Frame Relay detecta una situación de congestión, ésta situación es alertada a los nodos siguientes mediante este bit.
- **BECN (Backward Explicit Congestion Notification):** De la misma manera que son alertados los nodos siguientes, el nodo congestionado alerta a los nodos anteriores acerca de la situación, cambiando este bits, en las tramas "hacia atrás". De esta manera el nodo que origina el tráfico puede bajar su velocidad de transmisión, ayudando a descongestionar la red.
- **DE (Discard Eligibility Indicator):** Cuando la red Frame Relay está congestionada, es necesario descartar tramas. Las primeras tramas a descartar serán las que tengan encendido el bit "DE". Este bit es "encendido" por los nodos de entrada de la red Frame Relay en función del "CIR" (Ver 5.1.3) contratado por el cliente. Todas las tramas que excedan el CIR contratado, son marcadas como "DE".

- **EA (Extension Bit):** Indica si el cabezal es de 2 o 4 bytes.

5.1.2 LMI (Local Management Interface)

A los efectos del intercambio de información entre los equipos del prestador de servicio y del cliente final, se ha desarrollado el protocolo "LMI". Este intercambio de información se utiliza para conocer el estado del enlace y los PVC configurados en el mismo. Este protocolo es opcional dentro de las recomendaciones de Frame Relay, pero es habitual que esté implementado en las casi todas las implementaciones.

El intercambio de información entre equipos se implementa mediante el uso de tramas especiales de administración, que disponen de números de DLCI reservados para estos fines. Estas tramas chequean el status de la conexión y proveen la siguiente información:

- Indicación de que la interfaz está activa ("keep alive")
- Los DLCIs definidos en la interfaz
- El status de cada circuito virtual, por ejemplo, si está congestionado o no.

Existen tres versions de LMI:

- **LMI:** Frame Relay Forum Implementation Agreement (IA), FRF.1 superceded by FRF.1.1
- **Annex D**: ANSI T1.617
- **Annex A:** ITU Q.933 referenced in FRF.1.1

Si bien el término LMI es usado comúnmente para referirse al FRF.1 IA, puede ser usado como término genérico para cualquiera de los 3 protocolos. Cada uno de los protocolos incluye pequeñas diferencias en el uso e interpretación de las tramas de control, por lo que es importante que los equipos del proveedor de servicio estén configurados con el mismo protocolo que los equipos locales.

5.1.3 La contratación de Frame Relay (CIR)

Los servicios públicos Frame Relay se comercializan teniendo en cuenta varios parámetros, entre los que el "CIR" (Committed Information Rate) es el más importante. El CIR es la velocidad media de transmisión acordada entre el cliente y el proveedor de servicio. Es un parámetro que se establece en forma independiente para cada PVC.

En una configuración típica, un "nodo central" puede tener un enlace con el prestador de servicios sobre el que se configuran varios PVC, hacia los "nodos secundarios", o sucursales. El enlace físico puede ser, por ejemplo, de 1 Mb/s, y cada PVC puede tener un CIR, por ejemplo, de 64 kb/s.

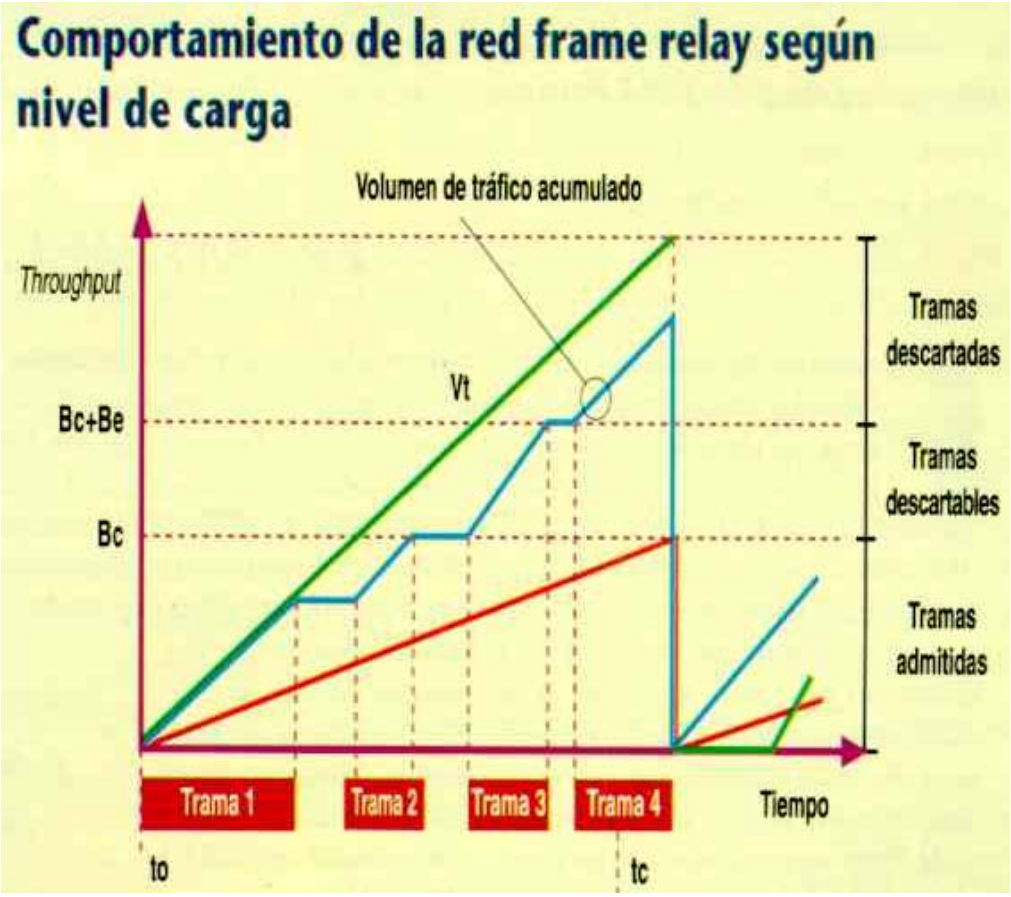
Esto significa que la *velocidad media* de transmisión entre el nodo central y los nodos secundarios debe ser 64 kb/s (CIR), aunque la velocidad física de cada trama será de 1 Mb/s.

La velocidad media, se mide sobre un tiempo prefijado, llamado generalmente $\mathbf{t_c}$ (generalmente 1 segundo). En el tiempo t_c, el cliente se compromete a no pasar más de **Bc** bits, equivalentes al CIR x t_c kb para un determinado PVC.

$$Bc \text{ (Committed Burst Size)} = CIR \times t_c$$

Se establece también un tráfico de exceso, llamado generalmente **Be** (Excess Burst Size). Las tramas enviadas por el cliente dentro de un t_c que excedan Bc bits, serán marcadas por el proveedor de servicio como "descartables" (Bit "DE" del cabezal de la trama, ver 5.1.1). Estas serán las primeras tramas a descartar en caso de que exista congestión en la red Frame Relay.

Las tramas que dentro del mismo intervalo t_c excedan Bc + Be serán directamente descartadas en la entrada de la red Frame Relay.



Para los interesados en profundizar en Frame Relay, se recomienda la lectura de "The Basic Guide to Frame Relay Networking" [13].

5.2 ATM

ATM (Asynchronous Transfer Mode) surgió como respuesta a la necesidad de tener una red multiservicio que pudiera manejar velocidades muy dispares. Técnicamente puede verse como una evolución de las redes de paquetes. Como otras redes de paquetes (X.25, Frame Relay, TCP/IP, etc.) ATM integra las funciones de multiplexación y conmutación. A su vez está diseñada para soportar altos picos de tráfico y permite interconectar dispositivos que funcionen a distintas velocidades. ATM está especialmente diseñada para soportar aplicaciones multimedia (voz y video, por ejemplo).

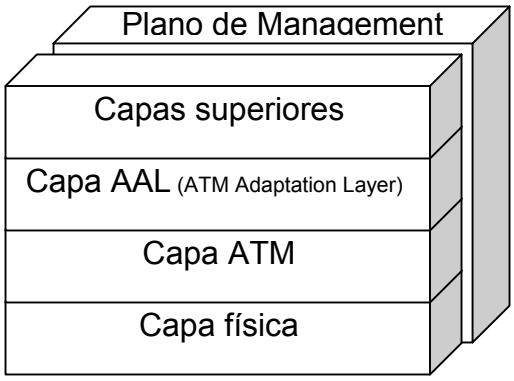
Si bien ATM puede ser usada como soporte para servicios dentro las redes de área locales, en usuarios finales, su principal protagonismo ha estado en las redes de "backbone" de los proveedores de servicios públicos.

Los protocolos de ATM están estandarizados por la ITU-T, y con especial contribución del "ATM Forum". El "ATM Forum" es una organización voluntaria internacional, formada por fabricantes, prestadores de servicio, organizaciones de investigación y usuarios finales.

Algunas de las ventajas de ATM frente a otras tecnologías son:

- Alta performance, realizando las operaciones de conmutación a nivel de hardware
- Ancho de banda dinámico, para permitir el manejo de picos de tráfico
- Soporte de "clase de servicio" para aplicaciones multimedia
- Escalabilidad en velocidades y tamaños de redes. ATM soporta velocidades de T1/E1 (1.5 / 2 Mb/s) hasta STM-16 (2 Gb/s)
- Arquitectura común para las redes de LAN y WAN

De forma similar al modelo OSI (Ver 3) ATM también está diseñada en un modelo de capas. En el caso de ATM, el modelo de capas puede verse en varios "planos", como se esquematiza en la figura



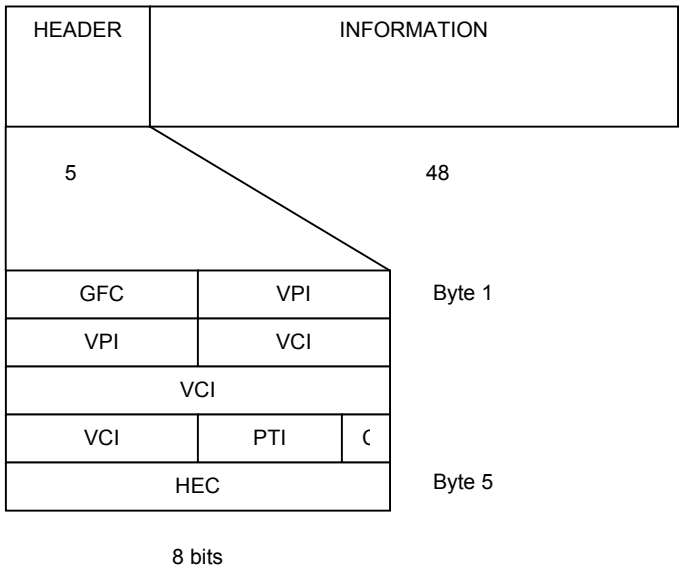
A continuación se describen las Capas físicas, ATM y AAL. Para una mejor comprensión, se comienza describiendo la capa ATM, luego la AAL y por último la capa Física.

5.2.1 Capa ATM

La Capa ATM es la responsable de transportar la información a través de la red. ATM utiliza "conexiones virtuales" para el transporte de la información. Estas conexiones virtuales, pueden ser permanentes (PVC) o del tipo "llamada a llamada" (SVC).

5.2.1.1 Celdas ATM

Para poder manejar los requerimientos de tiempo real, se optó por usar unidades de tamaño fijo y pequeño. Estas unidades, llamadas celdas, contiene 48 bytes de información y 5 bytes de "cabecera". Este tamaño fijo y pequeño asegura que la información de tiempo real, como el audio y el video no se vea afectada por la duración de tramas o paquetes largos (recordar que Ethernet o Frame Relay, permiten paquetes de más de 1.500 bytes). La siguiente figura muestra la estructura del cabezal de las tramas ATM, que contiene los siguientes campos:



- **GFC (Generic Flow Control):** Es usado únicamente en conexiones que van desde un usuario final hasta el primer nodo ATM de una red pública (UNI = User to Network Interface), como control de flujo entre el usuario y la red. En conexiones entre nodos ATM de la red pública (NNI = Network to Network Interface), no se utiliza este campo.
- **VPI (Virtual Path Identifier):** Al igual que Frame Relay, ATM brinda servicios orientados a la conexión, basados en circuitos virtuales permanentes (PVC) o temporales (SVC). El campo VPI contiene el identificador del camino virtual al que pertenece la trama

- **VCI (Virtual Channel Identifier):** Dentro de un mismo camino virtual (identificado por el VPI), pueden establecerse varios canales o circuitos virtuales (VCC). El campo VCI identifica cada circuito o canal virtual dentro del camino virtual.
- **PTI (Payload Type Indicator):** Indica el tipo de datos o información que transporta la celda en los 48 bytes de "Información". Es de hacer notar que este campo no siempre transporta "datos", sino que algunas cedas utilizan este campo para enviar información de señalización, mensajes administrativos de la red, etc.
- **CLP (Cell Loss Priority):** Es utilizado como marca de prioridad de la celda o trama. En caso de congestión, la red puede descartar los paquetes de menor prioridad (CLP = 1). Las celdas marcadas con CLP = 0 se consideran de alta prioridad y no deberían ser descartadas.
- **HEC (Header Error Control):** Es un byte de control de errores en el cabezal. Únicamente se realiza control de errores sobre el cabezal. El algoritmo utilizado permite corregir errores en 1 bit

5.2.2 Capa AAL (ATM Adaptation Layer)

La capa AAL realiza el "mapeo" necesario entre la capa ATM y las capas superiores. Esto es generalmente realizado en los equipos terminales, en los límites de las redes ATM.

La red ATM es independiente de los servicios que transporta. Por lo tanto, la "información" de cada celda es transportada en forma transparente a través de la red ATM. La red ATM no conoce la estructura ni procesa el contenido de la información que transporta. Por ello es necesario, en los límites de la red ATM, una capa que adapte los diversos servicios o protocolos a transportar, a las características de la red ATM. Esto es realizado por la capa AAL.

A los efectos de las funciones de la capa AAL, es necesario categorizar los servicios a transportar por ATM según los siguientes ítems:

- **Relaciones de tiempo entre fuente y destino:** Indica si el reloj de destino debe "sincronizarse" con el reloj de la fuente
- **Velocidad (bit-rate):** Indica si se trata de servicios de velocidad constante o variable
- **Modo de conexión:** Orientado a la conexión o No orientado a la conexión

Como resultado, se han definido 4 "clases de servicios", denominadas A, B, C y D, como puede verse en la siguiente tabla:

Clase	A	B	C	D
Relaciones de tiempo entre fuente y destino	Requerido		No Requerido	
Bit-Rate	Constante	Variable		
Modo de Conexión	Orientado a la conexión			No orientado a la conexión

Para cada "clase de servicio" se ha implementado una capa AAL, las que se conocen como AAL-n, como se verá más adelante.

Las capas AAL-n, a su vez, se subdividen en dos sub-capas:

- **Convergence Sublayer (Sub-capa de convergencia):** Se encarga de las adaptaciones específicas que requiere cada clase de servicio.
- **Segmentation and Reassembly Sublayer (Sub-capa de segmentación y reensamblado):** Se encarga de dividir la información para poder transmitirla en las pequeñas celdas de ATM y luego reensamblarla en el destino

5.2.2.1 AAL - 1

Se utiliza para la clase de servicio A (servicios orientados a la conexión, de velocidad constante y que requieren referencia de tiempos para sincronización del destino con la fuente)

Se utiliza para transporte de servicios sincrónicos (por ejemplo, servicios sincrónicos de 64 kb/s) o asincrónicos de velocidad constante (por ejemplo, líneas E1 de 2 Mb/s).

5.2.2.2 AAL - 2

Se utiliza para la clase de servicio B (servicios orientados a la conexión, de velocidad variable y que requieren referencia de tiempos para sincronización del destino con la fuente).

Ha sido la más difícil de desarrollar, debido a la dificultad de recuperar en el destino el reloj de referencia de la fuente cuando no se reciben datos por un periodo prolongado de tiempo. En AAL-1 esto no sucede, ya que los flujos de información son constantes.

Puede utilizarse, por ejemplo, para la transmisión de video comprimido. Esta aplicación envía "ráfagas" de información, generando tráfico impulsivo. MPEG-2, por ejemplo, tiene una relación de compresión de 10:1 en el peor caso. Sin embargo, si no hay cambios en la imagen de video, pueden llegarse a relaciones de compresión de hasta 50:1, generando largos periodos sin transmisión.

5.2.2.3 AAL – 3/4

Originalmente, la capa AAL-3 fue pensada para servicios orientados a la conexión y la AAL-4 para servicios no orientados a la conexión. Actualmente se han fusionado en la capa AAL-3/4, ya que las diferencias originales eran menores.

Se utiliza para la clase de servicio C y D (servicios de velocidad variable y que no requieren referencia de tiempos para sincronización del destino con la fuente). AAL-3/4 no utiliza todos los bytes de "información" de la celda ATM, lo que reduce el ancho de banda real apreciablemente

5.2.2.4 AAL – 5

Se utiliza para la clase de servicio C y D, al igual que AAL-3/4, pero utiliza todos los bytes de "información" de la celda ATM, optimizando por lo tanto el ancho de banda.

AAL-5 es conocida también como SEAL (Simple and Effective Adaptation Layer), ya que no provee secuenciamiento ni corrección de errores, sino que delega estas tareas en las capas superiores.

5.2.3 Capa Física

La capa física es responsable de transmitir los datos sobre un medio físico, de manera similar a la capa física del modelo de referencia OSI.

El medio de transporte puede ser eléctrico u óptico. ATM es generalmente transportado sobre SDH (Synchronous Digital Hierarchy).

Las velocidades típicas son de 155.520 kb/s (155 Mb/s) o 622.080 kb/s (622 Mb/s), acuerdo a la recomendación I.432

5.3 Routers

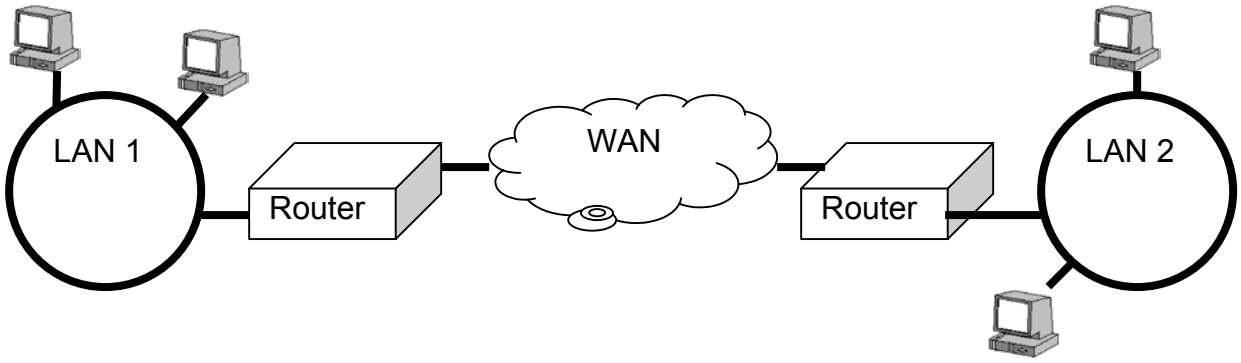
Como se mencionó en al principio de éste capítulo (Ver 5), la función de las redes WAN es interconectar redes LAN distantes entre sí, a través de enlaces públicos o privados, generalmente de baja velocidad en comparación con la velocidad de las redes LAN. En las secciones anteriores se estudiaron los protocolos Frame Relay (Ver 5.1) y ATM (Ver 5.2), el primero como ejemplo de protocolo típico de WAN y el segundo como ejemplo de protocolo de back-bone de los prestadores de servicios.

Para poder interconectar redes LAN distantes, mediante algún protocolo de WAN, es necesario disponer de equipos de "interconexión", que cumplan varias funciones, entre las que se destacan:

- Posibilidad de rutear tráfico, para disminuir el tráfico de WAN no deseado (Broadcast, etc.)
- Posibilidad de manejar protocolos de LAN y de WAN.

Estos equipos se conocen normalmente como “Routers”. Si bien el nombre indica, en principio, que el equipo debe poder “rutear” paquetes (es decir, trabajar a nivel de capa 3 en el modelo OSI), también se espera de estos equipos (por lo menos para los equipos diseñados para las corporaciones) que soporten varios protocolos de WAN (como Frame Relay, por ejemplo).

Un Router corporativo típico debe disponer, por lo tanto, y como mínimo, de un “puerto de LAN” y un “puerto de WAN”. Asimismo, debe poder rutear los protocolos más comunes de LAN (típicamente IP, aunque aún varias redes LAN utilizan IPX), enviando únicamente los paquetes que correspondan al puerto WAN y debe implementar varios protocolos de WAN (como Frame Relay, X.25, etc.)



Para poder implementar las funciones de ruteo, los Routers deben disponer de “tablas de ruteo”. Estas tablas pueden estar definidas en forma estática, por un administrador, o pueden generarse en forma automática, ya que los routers disponen de protocolos propios de “descubrimiento de rutas”. Estos protocolos, que implementan el intercambio de información de rutas entre varios Routers, se llaman habitualmente “protocolos ruteo”. Los más comunes son los llamados RIP y OSPF (ambos están estandarizados, de manera que routers de diversas marcas pueden coexistir en una misma red).

6 Tecnologías de acceso xDSL

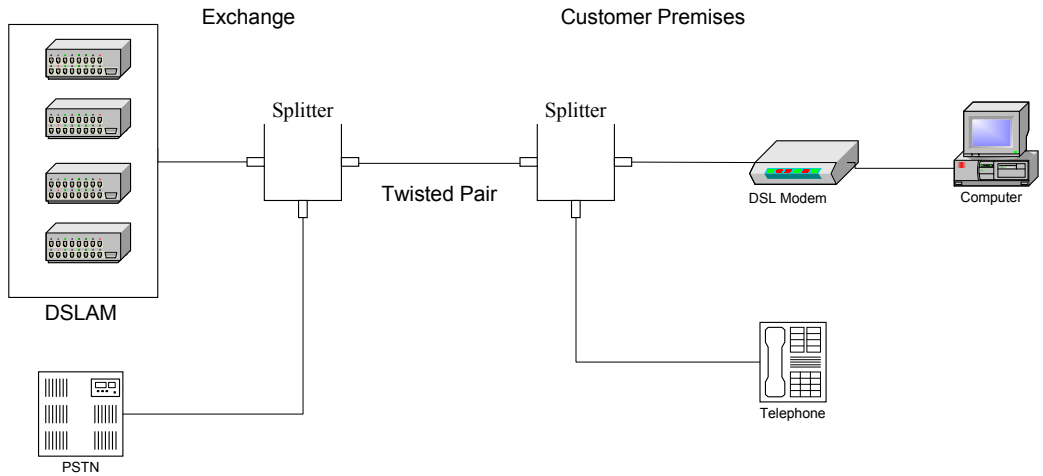
Las redes WAN requieren conexiones digitales desde las oficinas de las empresas hasta las oficinas de los prestadores de servicios, las que pueden estar alejadas varios kilómetros.

La interconexión desde los prestadores de servicios a las empresas puede realizarse mediante enlaces inalámbricos, o mediante el tendido de cables de cobre o fibras ópticas. Gran parte de las empresas prestadoras de servicios de datos son las mismos que las prestadoras de servicios telefónicos, y ya disponen de cables tendidos hasta las oficinas de las empresas. Estos son generalmente cables de cobre, pensados originalmente para brindar servicios telefónicos. A los efectos de minimizar los costos, se han desarrollado técnicas que permiten utilizar estos mismos cables de cobre para brindar servicios digitales. Estas tecnologías se conocen “Digital Subscriber Loop” o bucle digital de abonado. Entre estas tecnologías se encuentran ADSL, HDSL, VDSL y otras [14]. En forma genérica, todas ellas se engloban dentro de las tecnologías conocidas como xDSL.

Todas las tecnologías xDSL permiten comunicación de datos en forma bidireccional. Sin embargo, algunas son “asimétricas” y otras “simétricas”, en lo que respecta a las velocidades de transmisión de datos en cada sentido.

6.1 ADSL

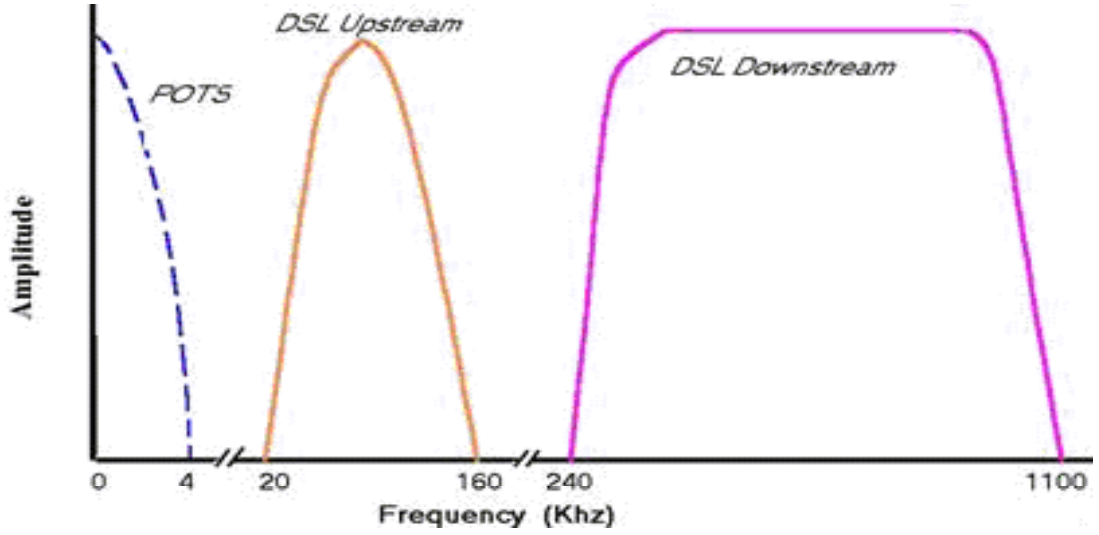
ADSL, o “Asymmetric Digital Subscriber Loop” [15] (DSL asimétrico), brinda una conexión digital con velocidades de “subida” y de “bajada” diferentes. Está pensada típicamente para servicios de acceso a Internet, en los que, por lo general, es mucha más la información que debe viajar desde Internet hacia la empresa que desde la empresa hacia Internet. Por ejemplo, al navegar sobre la web, un usuario realiza un clic (envío muy pequeño de información), y “baja” una página completa (envío importante de información).



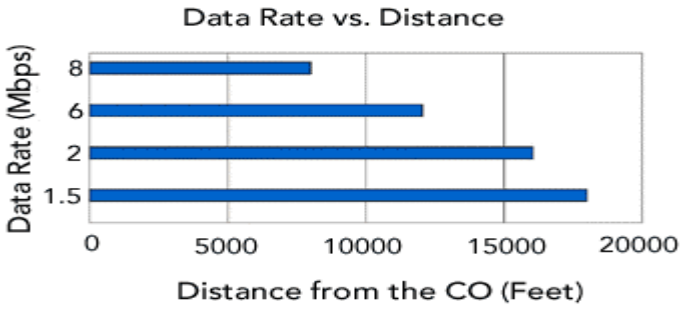
Los servicios ADSL pueden ser brindados a diferentes velocidades de “subida” y “bajada”. La tecnología admite hasta 7 Mb/s de “bajada” y 928 kb/s de “subida”.

Como todas las tecnologías DSL puede ser brindada sobre los pares telefónicos existentes. Sin embargo, ADSL permite utilizar el mismo par sobre el que funciona un servicio telefónico. Es decir, sobre un mismo par telefónico pueden coexistir un servicio telefónico analógico y un servicio de datos ADSL.

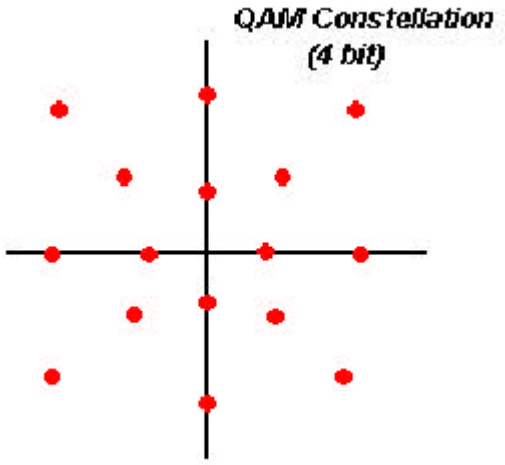
Para lograr esto, ADSL utiliza modulación en frecuencias supra-vocales, y separadores o “splitters” en las oficinas donde se presta el servicio. Estos “splitters” separan el servicio telefónico del servicio de datos. El servicio telefónico es conectado a un teléfono analógico, y el servicio de datos a un MODEM DSL. Generalmente este MODEM dispone de una puerta LAN (RJ45) para ser conectado directamente a la red de datos del cliente.



Las distancias entre prestador y cliente a las que funciona ADSL dependen de la velocidad contratada, y pueden llegar hasta los 5 km.



ADSL utiliza modulación DMT (Discrete Multitone Modulation). Esta modulación consiste en dividir la banda de frecuencias disponibles en 256 sub-bandas, o canales, separados 4 kHz. 32 de estos canales se utilizan para subida, y el resto para bajada. Cada canal envía información en forma independiente, utilizando modulación QAM (Quadrature Amplitude Modulation), en una "constelación" de 2^n puntos. Cada punto representa un conjunto de n bits, los que se envían en un único símbolo modulando en amplitud y fase una portadora.



Una de las características de DMT es que permite que cada canal o sub-banda utilice constelaciones más o menos densas (es decir, con más o menos puntos), de acuerdo al ruido existente. Los modems ADSL pueden ajustar dinámicamente, de acuerdo a las condiciones de ruido existentes, las constelaciones a utilizar en cada canal

6.2 ADSL Light o G.Light

La tecnología ADSL Light [16] es similar a la ADSL, pero no requiere de "splitter" o separador en las oficinas donde se presta el servicio. Es conocida también como "splitterles DSL". La tecnología fue pensada para brindar servicios a los hogares, dónde la simplicidad de instalación es un factor de especial importancia.

Dado su público objetivo, la velocidad de transmisión máxima fue diseñada en 1.5 Mb/s, permitiendo equipos terminales más sencillos, y por lo tanto, más baratos.

Dado que no hay splitter, los problemas de interferencia se ven acentuados, pero por lo general no son problema en las velocidades en que trabaja G.Light. En algunos casos es necesario instalar "microfiltros" en teléfonos, para eliminar posibles ruidos.

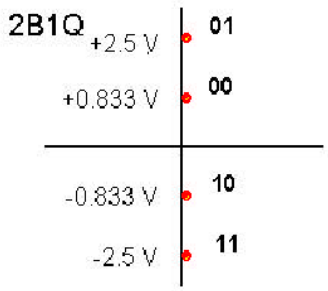
6.3 HDSL

HDSL, o “High Speed Symmetric Digital Subscriber Loop” [17] (DSL simétrico de alta velocidad), brinda una conexión digital con iguales velocidades de “subida” y de “bajada”. Está pensada típicamente para servicios 1.5 y 2 Mb/s, típicamente de tipo T1 o E1.

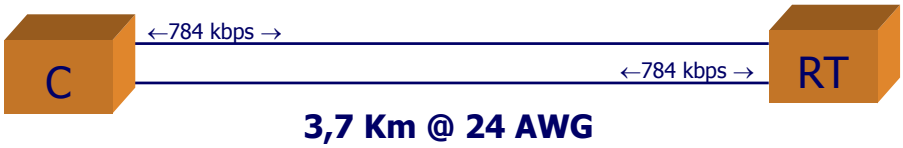
HDSL utiliza dos pares de cobre, y fue diseñada para que la gran mayoría de los cables tendidos originalmente para servicios telefónicos, puedan servir de soporte para éste nuevo servicio digital. Ambos pares son bidireccionales, y funcionan a la mitad de la velocidad de transmisión total.

A diferencia de ADSL, los pares deben ser dedicados. No se pueden compartir otros servicios sobre los mismos pares por los que se brindan servicios HDSL

HDSL utiliza modulación 2B1Q, codificando 2 bits en cada símbolo.



La distancia a la que puede funcionar correctamente un servicio HDSL depende de los diámetros de cable utilizados, la cantidad de empalmes, y otros factores ambientales. Típicamente puede llegar a 3.7 km, con cables 24 AWG



6.4 HDSL2

HDSL2 [18] es una mejora a HDSL, que permite las mismas funciones, pero utilizando solamente un par de cobre.

7 Administración de Redes

Junto con el crecimiento de las redes de datos, surgió la necesidad de su administración. La administración de redes incluye las tareas de diseño, integración y coordinación de los equipos de hardware, los programas de software y los recursos humanos necesarios para monitorear, testear, configurar, analizar, evaluar y controlar la red y sus recursos a los efectos de lograr la calidad de servicio requerida.

Desde el punto de vista corporativo, las tareas de administración de redes deben basarse en obtener en forma predecible y consistente una calidad de servicio adecuada a las necesidades, a un costo aceptable para la corporación.

Para poder realizar las tareas de administración, es necesario poder detectar fallas, aislarlas y corregirlas, al menor costo y en el menor tiempo posible. Es necesario también poder realizar cambios en las configuraciones afectando lo mínimo posible al servicio. Una buena administración de red se basa en prever, en la medida de lo posible, posibles puntos de falla, y evitarlos antes de que sucedan. Esto se basa en tener medidas de utilización de la red, analizarlas y tomar acciones preventivas antes que correctivas.

Varios organismos han trabajado en intentar estandarizar las tareas relacionadas a la administración de las redes, entre ellos la ISO, el ITU-T y el IETF. Cada uno de ellos ha establecido normas y recomendaciones, viendo a la administración de las redes desde su propia óptica.

La ISO ha establecido los criterios generales en la recomendación 7498-4 [19]. Dentro de la administración de redes, se distinguen 3 componentes que han sido estandarizados: La estructura de la información (10165-x), los protocolos a utilizar (9595 y 9596) y las funciones propias de la administración (10164-x, conocidas generalmente como “FCAPS”)

Por su lado, la ITU-T, con su visión centrada en su historia telefónica, ha desarrollado los estándares para lo que se ha dado a llamar “TMN”, o “Telecommunications Management Network” (Red de gerenciamiento de telecomunicaciones) [20] . La estructura general de esta red, se describe en las recomendaciones M.30xx. La primer versión de esta serie de recomendaciones fue publicada en 1989 (en ese momento por la CCITT) [21]. La versión conocida actualmente como M.3010 fue publicada en 1992, y revisada en 1996 [22]. Al igual que la ISO, se distinguen 3 componentes de las TMN: Estructura de la información (M.31xx), Protocolos (Q.8xx) y las funciones propias de la administración (M.32xx, M.3300, M.3400).

Finalmente, el IETF ha desarrollado un sistema pragmático, mucho más sencillo, aunque también más limitado. Las recomendaciones acerca de la estructura general se han publicado en los RFC 1052 y 1155, y se presentan 2 componentes estandarizados: La estructura de la información (RFC1113 , MIB) y los protocolos (RFC 1157, SNMP).

7.1 Funciones a considerar en la administración de redes según ISO

Vamos a detenernos en las funciones de la administración, definidas por ISO, llamadas comúnmente “funciones FCAPS”, debido a sus siglas en inglés.

7.1.1 Gestión de Fallas (Fault Management)

Una de las funciones de administración de redes es poder detectar y resolver fallas. El propósito de la gestión de fallas es asegurar el correcto funcionamiento de la red y la rápida resolución de las fallas que se presenten.

La gestión de fallas comienza por la detección de las mismas, ya sea en forma automática o en reportadas por los usuarios. Es recomendado disponer de un sistema de “registro y seguimiento”, que permita dejar registrado el incidente, y las acciones realizadas para su resolución.

La resolución de fallas debe generar conocimiento, para prevenir fallas futuras. Muchas veces es difícil realizar un análisis profundo de las causas durante el momento en que la falla está presente, sobre todo si la falla afecta considerablemente al servicio. Las presiones de los usuarios (y sobre todo de “sus jefes”), llevan muchas veces a tratar de solucionar lo más rápidamente posible la falla, sin detenernos a buscar sus causas. Si bien la búsqueda y análisis de las causas puede generar demoras adicionales en la resolución de los problemas, muchas veces es preferible esto a que la misma falla se repita una y otra vez sin entender por que sucede.

Como parte de la gestión de fallas es necesario disponer de un “plan de contingencia”, planificado y documentado, que nos permita brindar servicios (quizás en forma reducida), mientras se resuelve la falla e investiga sus causas

También se debe disponer de un plan de gestión de alarmas, con procesos acordes a su criticidad.

7.1.2 Gestión de Configuración (Configuration Management)

Para poder gestionar las redes, es necesario saber qué elementos se disponen, cómo están iterconectados, cual es la configuración específica de cada uno de los elementos, etc. La gestión de la configuración consiste en mantener esto en forma ordenada y documentada.

Se debe partir de una descripción de la red y cada uno de sus componentes. A quien le prestan servicio, con que características, etc. Esto puede llevarse a cabo en varios niveles.

Por ejemplo, parte de la gestión de configuración, podría ser disponer de un “plano” de las centrales telefónicas empresariales (PBX), con cada una de sus componentes (placas, internos, líneas, etc.), a que está conectado cada puerto, que facilidades tiene programado cada interno, etc.

Deben preverse mecanismos para los agregados, mudanzas y cambios, de manera que se afecte mínimamente al servicio, y que los cambios queden documentados.

El mantenimiento de la documentación debe incluir todo lo necesario como para comprender la arquitectura de la red y cada uno de sus componentes. Esto incluye inventarios, diagramas de conexiones, cableado, configuraciones, planes de numeración, planes de direcciones de red, etc.

7.1.3 Gestión de Costos (Accounting)

Las redes de telecomunicaciones tienen costos asociados. Desde la amortización de los equipos, pasando por los costos de utilización de servicios, hasta los propios costos del gerenciamiento.

En general, podemos separar los costos en 3 categorías:

- **Costos directos de las telecomunicaciones:** Corresponden a los costos del uso de las redes. Estos costos tienen generalmente un componente fijo y un componente variable. Por ejemplo, un prestador de servicio de acceso a Internet puede cobrar una tarifa plana mensual, y un prestador de telefonía de larga distancia puede cobrar una tarifa según cada llamada realizada.
  Dentro de los costos directos se deben incluir todos los costos de telecomunicaciones:
  - Servicios de datos
  - Líneas directas
  - Costos de llamadas telefónicas
  - Costos de servicios telefónicos (Colectivos, facilidades como CallerID, etc)
  - Etc
- **Costos de equipos:** Los equipos de telecomunicaciones pueden ser propios o arrendados. En el caso de tener equipos propios, existe un costo de amortización, generalmente prorrateado en un período estimado como el de vida útil del equipo. Los equipos arrendados tienen un costo mensual prefijado.
- **Costos del Gerenciamiento:** Todos los aspectos de gerenciamiento (FCAPS – Gestión de configuración, de fallas, de seguridad, de desempeño y la propia gestión de costos) tienen costos asociados. Ya sea que se dispone de personal propio, o que se subcontrate el servicio a terceros, existen costos de gerenciamiento. En el primer caso, estos costos están dados por los salarios del personal dedicado al gerenciamiento (administradores de red, help desk, etc.) En el segundo, los costos están dados por una cuota por servicios contratados a terceros.

Es usual que los costos se prorrateen entre “Centros de Costo”, generalmente asociado a sectores dentro de una Empresa (Ventas, Administración, Operaciones, etc.) En algunos casos, cada Centro de Costos tiene “cuotas”, de las que no puede excederse. Algunos sistemas pueden llegar a limitar el uso de ciertos servicios si se excede la cuota preestablecida.

7.1.4 Gestión de Desempeño (Performance Management)

La gestión del desempeño de las redes de telecomunicaciones tiene como objetivo asegurar el funcionamiento de las redes con la calidad de servicio deseada. Por ejemplo, que la cantidad de líneas urbanas que se dispone sea la adecuada, de manera que no exista congestión, que el ancho de banda en los enlaces entre sucursales sea suficiente para el tráfico cursado, etc.

Para lograr estos objetivos es necesario monitoreo ciertos parámetros de la red, que den un indicador acerca de la performance del servicio. Por ejemplo, si el servicio a monitorear es la disponibilidad de líneas urbanas salientes para realizar llamadas, un posible parámetro a monitorear puede ser la cantidad de líneas ocupadas en forma simultánea (para compararlo con la cantidad de líneas totales disponibles). Si el servicio a monitorear es el acceso a Internet, un posible parámetro a monitorear es el ancho de banda efectivamente utilizado (para compararlo con el ancho de banda disponible)

Estos parámetros son generalmente “de tiempo real”. Es decir, miden en un momento determinado el desempeño de un servicio. Si son consultados en forma periódica y almacenados, es posible realizar un control de la performance. Esto permite realizar reportes de gestión, ver su evolución en el tiempo, etc.

Analizando estos reportes es posible prever futuros problemas, dimensionar los recursos adecuadamente e incluso detectar fallas que pueden no afectar a un usuario en particular, pero si degradar la performance general del sistema (por ejemplo, si una línea urbana está rota, se disminuye la cantidad total de líneas disponibles y por lo tanto se degrada la performance, sin embargo, puede que nadie reporte el problema como tal).

A los efectos de gestionar el desempeño de las redes, cada equipo debe tener capacidad de medir los parámetros concernientes a sus servicios. Entre estos equipos se pueden encontrar PBX, Switches, Routers, Firewalls, etc.

7.1.5 Gestión de la Seguridad (Security Management)

La gestión de seguridad es un tema complejo en sí mismo. La seguridad en las redes de telecomunicaciones se enmarca dentro de los conceptos más generales de “Seguridad de la información”, que serán tratados más adelante.

Como conceptos generales, la gestión de la seguridad en las redes se debe encargar de definir permisos de acceso, controlar el fraude y prevenir los ataques.

El control de acceso debe definirse tanto para las redes de voz, como para las de datos. En las primeras, los controles típicos tienen que ver con los permisos para

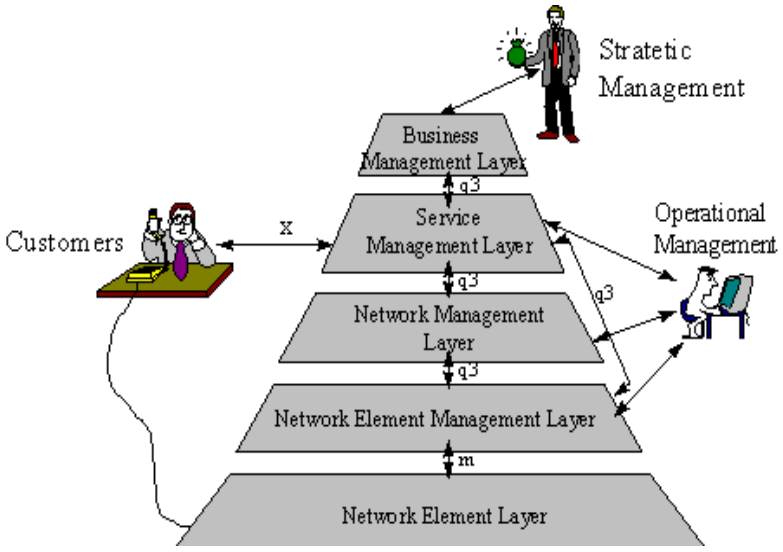
realizar determinado tipo de llamadas y con las facilidades a las que cada usuario tiene acceso. Por ejemplo, si un usuario puede escuchar las llamadas de otros, si puede desviar su teléfono a otros teléfonos, o a celulares, si se pueden realizar llamadas a número internacionales, o a 0900, etc. En las redes de datos, los controles típicos restringen el acceso a la información, ya sea interna o externa.

Los controles de fraude también deben realizarse en las redes de voz y datos. Fraudes típicos en redes de voz están relacionados con accesos a número prohibidos y llamadas "tandem". En las redes de datos los fraudes más comunes consisten en acceder a información restringida, ya sea desde dentro de la empresa, o desde fuera.

7.2 Funciones a considerar en la administración de redes según ITU-T

Las funciones se organizan en una estructura jerárquica de niveles que cubren todos los aspectos de gestión (en realidad, pensados para los prestadores de servicio) y clasifica las funciones que se deben realizar en cada nivel según criterios de responsabilidad. Los niveles son: el nivel de gestión de negocio, el nivel de gestión de servicio, el nivel de gestión de red y el nivel de gestión de elemento de red. Los niveles se representan habitualmente en forma de pirámide [23].

Entre cada nivel, se establecen "puntos de referencia", con interfaces estandarizadas. La primera versión de TMN establecía tres tipos de interfaces, llamadas Q1, Q2 y Q3. En versiones más recientes, se decidió unificar las interfaces Q1 y Q2 en una nueva interfaz Qx, y se mantuvo la interfaz Q3.



7.2.1 Gestión de Negocio (Bussines Management)

El nivel superior es el nivel de gestión de negocio que incluye los aspectos relacionados con las estrategias de negocio; en él se definen las acciones para conseguir el retorno de la inversión, aumentar la satisfacción de los accionistas de la compañía y de los empleados, etc. Las decisiones tomadas en este primer nivel definen los objetivos estratégicos de la compañía, y condicionan las funciones y procesos de la capa de nivel de gestión de servicio. Es decir, la gestión del servicio debe estar alineada con la estrategia de negocio definida en la corporación.

7.2.2 Gestión de Servicio (Service Management)

En la capa de gestión del nivel de servicio se decide cómo gestionar los servicios que se van a prestar en la red. En este nivel se incluyen todos los aspectos relacionados con la atención a los clientes o usuarios y los de desarrollo y operación de los servicios, y se realiza la gestión de las peticiones de servicio, la calidad del servicio —Quality of Service (QoS)—, la gestión de problemas, la facturación, etc.

7.2.3 Gestión de Red (Network Management)

Los servicios están soportados sobre las redes de telecomunicaciones. El nivel de gestión de red es responsable del transporte de la información entre dos extremos y de asegurar que ésta se realiza de forma correcta. Cualquier error o problema que se detecte en este nivel y que afecte a los servicios que se prestan a los clientes o usuarios debe ser notificado hacia el nivel de gestión de servicio.

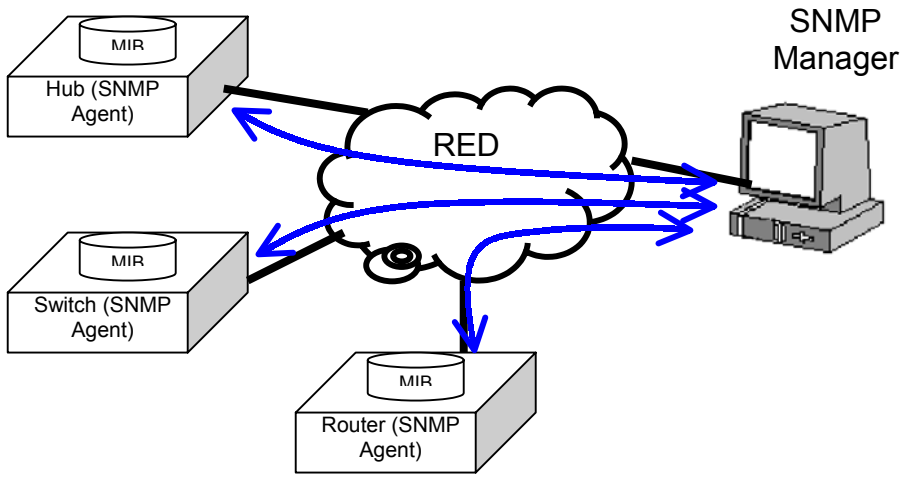
7.2.4 Gestión de Elementos de Red (Network Element Management)

Por último, el nivel de gestión de elemento de red se encarga de todos los aspectos relacionados con switches, sistemas de transmisión, etc., considerados como elementos aislados. Cualquier error o evento que se produzca en un equipo que pueda afectar al transporte de la información debe ser notificado hacia el nivel de gestión de red

7.3 SNMP

Para facilitar la administración de redes, el IETF (Internet Engineering Task Force) ha definido una recomendación llamada SNMP (Simple Network Management Protocol), que se ha convertido en un estándar en la industria de las comunicaciones.

SNMP (Simple Network Management Protocol) fue definido por el IETF (Internet Engineering Task Force) en 1989, en el RFC-1098 [24]. Desde entonces, se ha convertido en un estándar de la industria de las comunicaciones para controlar dispositivos de red desde estaciones de gerenciamiento y administración centralizadas.

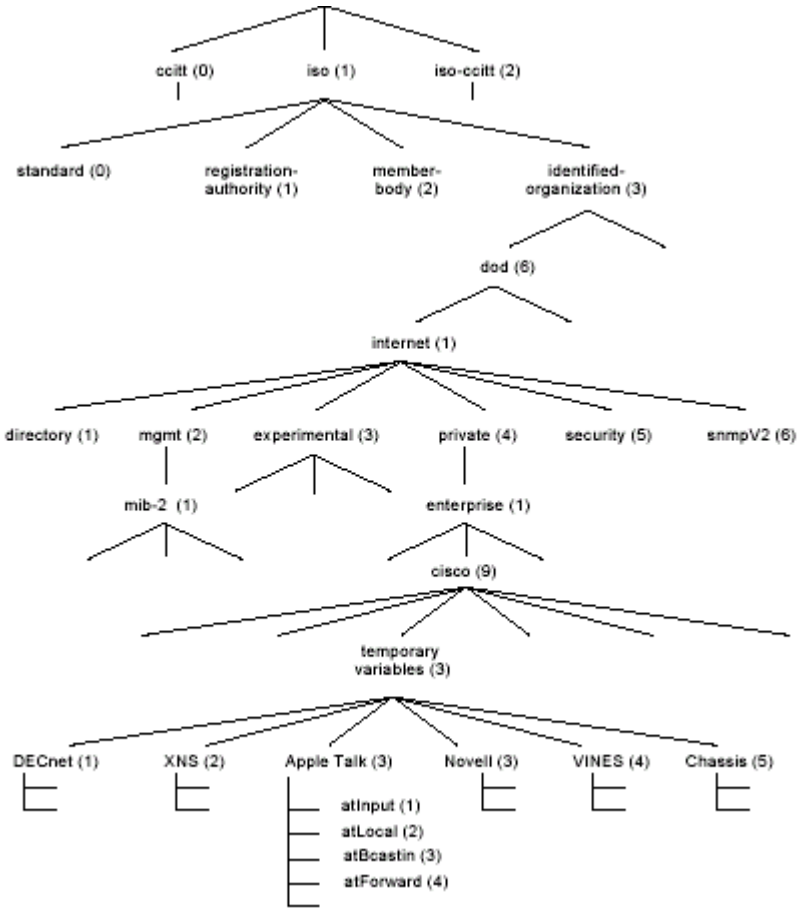


SNMP es un conjunto de protocolos y funciones especialmente diseñadas para la administración de redes, que utilizan el protocolo IP. SNMP permite a los administradores de red aislar fallas y monitorear el status y la performance de las redes de comunicaciones corporativas.

SNMP define dos componentes:

- **SNMP Manager:** Es una aplicación de software desde la que se realiza la administración, en forma centralizada, de la red.
- **SNMP Agent:** Residen en los diversos dispositivos de red (hubs, switches, routers, etc.) y generan información estadística acerca de sus funciones y recursos (por ejemplo, información estadística de tráfico). Esta información es almacenada en una base de datos local, llamada MIB (Management Information Base). A su vez, los “Agentes SNMP” pueden recibir y enviar información desde y hacia el “Administrador SNMP” (SNMP Manager), utilizando el protocolo UDP.

Cada “Agente SNMP” almacena la información que requiere en una base de datos llamada MIB (Management Information Base), cuyo formato está estandarizado.



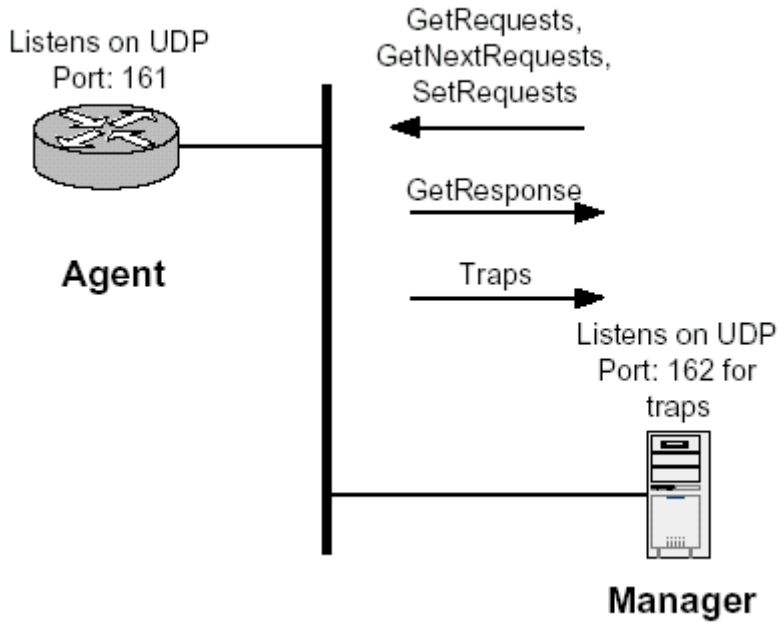
La información de la MIB está organizada en forma jerárquica. Cada elemento de información (llamado "objeto MIB") es una variable que almacena alguna característica o alguna información estadística del dispositivo administrado (Agente SNMP). Estos objetos MIB pueden ser escalares (es decir, contener un único valor), o tabulares (es decir, contener varios valores).

La estructura jerárquica de la MIB es en forma de "árbol", como se muestra en la figura. Cada objeto MIB está unívocamente identificado dentro de la jerarquía de la MIB, ya sea en una notación textual o numérica, indicando los diferentes nombres o números por los que se debe recorrer el árbol hasta llegar al objeto en cuestión. Por ejemplo, la variable "atInput" del ejemplo de la figura puede ser identificada como
"iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput" o por su equivalente numérico *"1.3.6.1.4.1.9.3.3.1".*

Cada fabricante tiene una "rama", bajo el objeto *"enterprise"*, y es libre de armar bajo esta rama la estructura de información que aplique mejor a sus productos.

Los agentes SNMP son controlados y monitoreados desde el administrador SNMP (SNMP manager) usando comandos simples, entre los que se destacan:

- **Read:** Es usado por el Manager para leer las variables del Agente (por ejemplo, para recolectar estadísticas de uso)
- **Write:** Es usado para configurar el equipo administrado. El Manager puede escribir ciertas variables de configuración del Agente
- **Trap:** Es utilizada en forma asíncrona por los agentes, para reportar eventos (típicamente fallas)



Existen tres versiones de SNMP, conocidas como SNMPv1 (versión 1) y SNMPv2 (versión 2) y SNMPv3 (versión 3). Todos ellas tienen un gran número de características similares, pero las versión más nuevas, ofrecen algunas mejoras frente a las anteriores. La versión 2 implementa los comandos "**GetBulk**" y "**Inform**". El comando GetBulk es usado por el SNMP Manager para recuperar en forma eficiente una gran cantidad de información de los agentes. El comando Inform es usado para intercambiar información entre varios SNMP Managers. La versión 3 introduce mejoras en la seguridad

Las distintas versiones SNMP son incompatibles entre sí, no solo por la incorporación de nuevos comandos, sino porque el formato de los mensajes intercambiados entre el Manager y los agentes es diferente en cada versión.

8 Seguridad de la Información

En todas las empresas, las redes de voz y datos transportan “información”. Esta información es valiosa para las organizaciones, al punto que se considera uno de sus “activos”. que, al igual que otros activos importantes para el negocio, tiene valor para la organización y consecuentemente necesita ser protegido apropiadamente.

Dentro de una corporación o empresa, la información puede existir en muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o medios digitales, mostrada en videos, o hablada en conversaciones. En muchos de estos aspectos, las redes corporativas participan activamente. Asegurar la información, incluye, por lo tanto, asegurar las redes por dónde la misma es transmitida.

Muchos componentes tecnológicos son utilizados en las redes corporativas asociados a los aspectos de seguridad. Sin embargo, todos ellos tienen como objetivo proteger *la información*, y no los componentes informáticos en si mismos. Tomando esto en cuenta, es natural ver a estos componentes tecnológicos, enmarcados dentro de los planes más genéricos de “seguridad de la información”.

8.1 Recomendaciones y normas relacionadas con la seguridad de la información

La “seguridad de la información” es un tema crítico para la gran mayoría de las corporaciones. Dado que el tema es genérico y no específico de una tecnología o tipo de negocio, varios organismos internacionales han desarrollado recomendaciones y estándares al respecto. La ISO ha publicado la recomendación 17799 [25], la que incluye un conjunto de prácticas acerca del gerenciamiento de la seguridad de la información.

La ISO 17799 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. La recomendación no cubre las problemáticas tecnológicas, sino que hace una aproximación al tema abarcando todas las funcionalidades de una organización en lo relacionado a la seguridad de la información.

Por su parte, la British Standards Institution, ha publicado las normas BS 7799. La parte 1 de esta norma es similar a la ISO 17799. La parte 2, conocida como BS 7799-2:2002 [26], es una norma enfocada a los procesos, y establece más que recomendaciones genéricas, reglas y requisitos a cumplir por las organizaciones. En su estructura es similar a las normas de calidad ISO 9001:2000, y al igual que éstas, es una norma “certificable”. Es decir, una empresa puede “certificarse” en el cumplimiento de la BS 7799-2:2002. Cabe destacar que la recomendación ISO

17799 no es una “norma certificable”, ya que incluye únicamente un “código de buenas prácticas” relativas a la gestión de la seguridad de la información. Es una guía que contiene consejos y recomendaciones que permite asegurar la seguridad de la información de la empresa.

Los requisitos establecidos en la BS 7799-2 se refieren a un Plan de Seguridad constituido por un “*Sistema de Gestión de Seguridad de la Información*” (SGSI), o en inglés, “*Information Security Management System*” (ISMS), en el que se aplican los controles de seguridad de la BS 7799-1 (y por lo tanto de la ISO 17799). Los requisitos que se establecen en el SGSI de la BS 7799-2 se pueden auditar y certificar. No hay versión ISO de la BS 7799-2.

La BS 7799-2:2002 esta basada en el enfoque de procesos, muy similar al de ISO 9001:2000.

Estos procesos tienen las siguientes etapas, las que se ejecutan en forma cíclica:

- **Planificar**
  Se planifica qué hacer y como hacerlos. A grandes rasgos, Esto incluye la definición del alcance del SGSI, las políticas generales de seguridad, la identificación y evaluación de los riesgos a los que está expuesta la información, y la preparación de los documentos preliminares

- **Hacer**
  Se ejecuta el plan, implementando los controles seleccionados, con el fin de cumplir los objetivos planteados

- **Verificar**
  Se verifica la ejecución del plan, implementando exámenes o controles periódicos (por ejemplo, auditorías). Se registran las desviaciones encontradas

- **Actuar**
  En base a las desviaciones encontradas o a las posibles mejoras al sistema se toman acciones correctivas o preventivas, las que llevan nuevamente a planificar, cerrando el ciclo.

En general, los objetivos de un SGSI es asegurar la continuidad del negocio y minimizar el daño ante un incidente de seguridad. En forma genérica, se establecen 3 objetivos de seguridad de la información:

- **Confidencialidad**
  Procurar que la información sea accesible sólo a las personas autorizadas a acceder a su utilización.

- **Integridad**
  Asegurar la exactitud y la completitud de la información y los métodos de su procesamiento

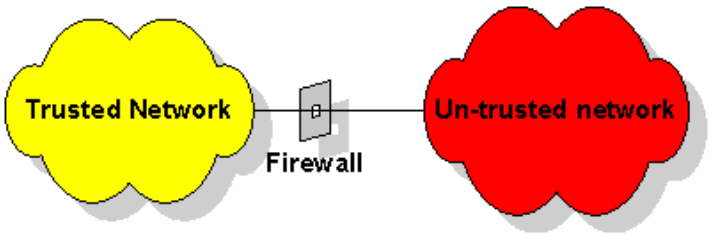
- **Disponibilidad**
  Asegurar que los usuarios autorizados tengan acceso a la información y los recursos asociados cuando lo requieran.

8.2 Tecnologías asociadas a la seguridad de la información

Hay un gran número de tecnologías asociadas a la seguridad de la información. El área de aplicabilidad de la seguridad es sumamente grande, al igual que las tecnologías y productos existentes. Dentro del tema “seguridad de la información” se enmarcan desde la criptografía, hasta los controles de acceso biométricos. En este capítulo nos concentraremos en solo algunas de las tecnologías existentes relacionadas con las redes de telecomunicaciones.

8.2.1 Firewall

Un “Firewall” o “Cortafuego” es un dispositivo o conjunto de dispositivos que restringe la comunicación entre dos o más redes. Sus funciones básicas consisten en bloquear tráficos indeseados y ocultar hacia el exterior la información interna [27]. Su utilización típica es separar a las redes internas (LAN, asumidas como “confiables” o “seguras”) de las redes públicas no seguras, como es el caso de Internet.



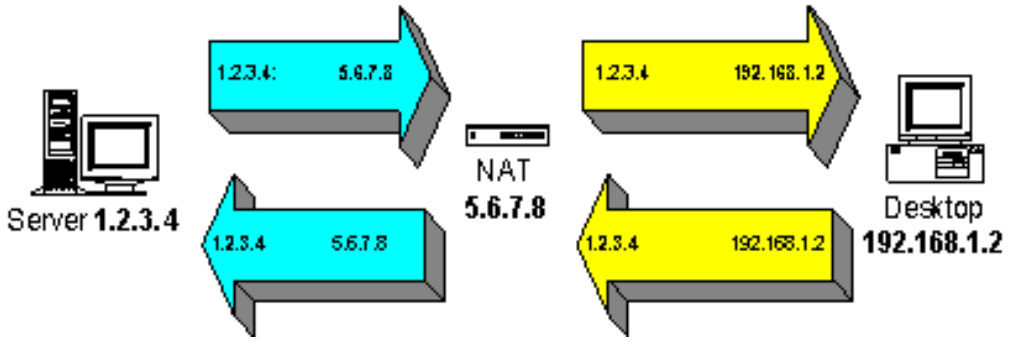
Actualmente la gran mayoría de las empresas tienen conexiones dedicadas hacia Internet. Esto trae aparejado por lo menos dos problemas. Uno de ellos tiene que ver con la "escasez" de direcciones IP "públicas". El otro está directamente asociado a los aspectos de seguridad.

NAT

Las direcciones IP públicas son limitadas, y están controladas por organismos internacionales. Cuando una empresa desea conectarse a Internet, típicamente recibe un conjunto reducido de direcciones IP públicas (generalmente una sola). Dado que por lo general se desea que todas (o un gran número) de las computadoras de la empresa tengan acceso a Internet, se debe compartir la IP pública entre un gran número de máquinas. Para resolver este problema se ha diseñado una solución conocida como **NAT** (Network Address Translation).

La implementación de NAT consiste en instalar un "gateway", o "pasarela", entre Internet y la LAN. Este "gateway" dispone de dos interfaces de red. Una de ellas conectada a la red pública (quien tiene asignada la IP pública) y la otra conectada a la LAN (con una dirección IP privada). Todos los paquetes que entran o salen desde la LAN a Internet, pasan por este "gateway". Cuando, por ejemplo, una computadora de la LAN (interna) envía un paquete a Internet, el "gateway NAT" reemplaza la dirección IP privada del PC de origen, por su propia dirección IP pública. Asimismo, registra en su memoria la dirección IP interna (origen) y la dirección IP externa y el número de puerto (destino).

El servidor remoto, recibe un paquete que contiene como origen la dirección IP pública del "gateway NAT" (es decir, la única dirección IP pública de la Empresa), y dirige su respuesta a esta IP. Cuando esta respuesta es recibida por el "gateway NAT", éste revisa en sus tablas almacenadas en memoria cual es la dirección IP interna a la que debe enviar esta respuesta (en base a la IP y puerto desde donde recibe el paquete de respuesta). Una vez obtenida la IP interna, sustituye la IP de destino del paquete, y envía el mismo hacia la LAN



La mayoría de los Firewalls implementan NAT, como tecnología de acceso a Internet, y como primer medida de seguridad. NAT deja las direcciones internas

(privadas) ocultas hacia Internet. Sin embargo, hay que hacer notar que NAT funciona únicamente cuando el origen de la comunicación es interno.

Por lo general, las empresas deben recibir también tráfico originado en Internet. Por ejemplo, si se dispone de un servidor de correo electrónico, los correos entrantes llegan desde Internet hacia la Empresa. Lo mismo sucede con las páginas web, servidores FTP, etc.

Es decir, por lo general no es posible bloquear totalmente el tráfico desde Internet hacia las Empresas, ya que esto impediría el funcionamiento de varios servicios esenciales.

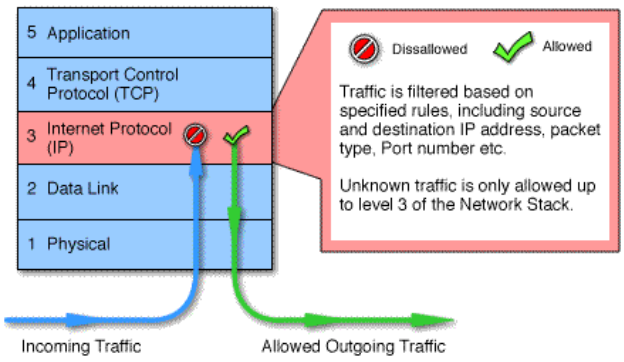
A los efectos de aumentar la seguridad, tanto en el tráfico entrante como en el tráfico saliente, los Firewall implementan varios tipos de "inspecciones" en los paquetes que pasan (o intentan pasar) de Internet a la LAN y viceversa.

Packet Filter

Un Firewall que implementa "filtrado de paquetes", inspecciona cada paquete IP, y lo evalúa a los efectos de determinar si puede o no pasar. En este caso, la decisión es hecha paquete a paquete, sin importar los paquetes recibidos anteriormente. Los bloqueos se pueden definir en base a direcciones de origen y destino, tipo de paquete, etc.

Este tipo de filtrado es sencillo de implementar, pero es relativamente pobre en sus características, ya que permite bloquear completamente o permitir el paso abiertamente.

Los Firewall que implementan filtrado de paquetes, trabajan a nivel de la capa 3



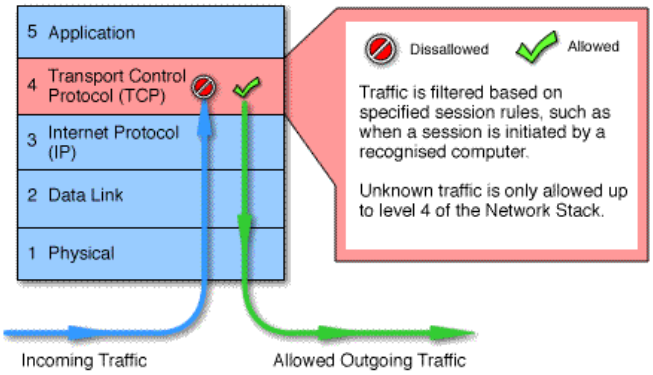
Stateful Inspection

Una manera mas sofisticada de filtrar paquetes consiste en tener en cuenta no solo el paquete actual, sino la "historia", de manera que el paquete se considere

en el contexto de los paquetes anteriores. Esto permite distinguir entre conversaciones establecidas y nuevas conversaciones, y tomar decisiones acordes.

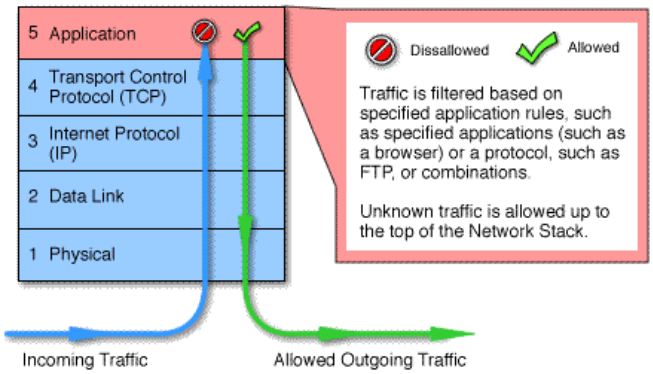
Circuit Level

Si se inspecciona hasta la capa 4, es posible identificar sesiones, y por lo tanto, permitir solo sesiones iniciadas por computadores conocidos.



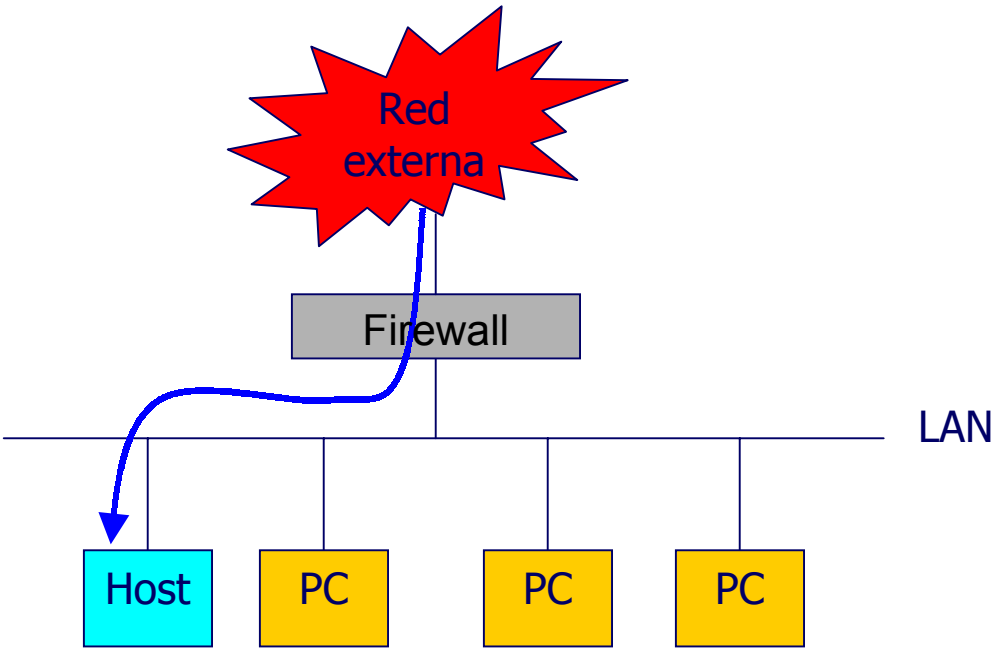
Application Level

Llegando hasta la capa 5, se pueden implementar filtros por aplicación. Por ejemplo, se pueden distinguir paquete http:post, http:get, etc.
Los Firewall que implementan filtros en la capa de aplicación requieren por lo general de un alto nivel de mantenimiento y actualización, ya que los fabricantes deben mantener al día el filtrado de nuevas aplicaciones o protocolos. Como contrapartida, son mas seguros que el resto de los tipos de Firewall

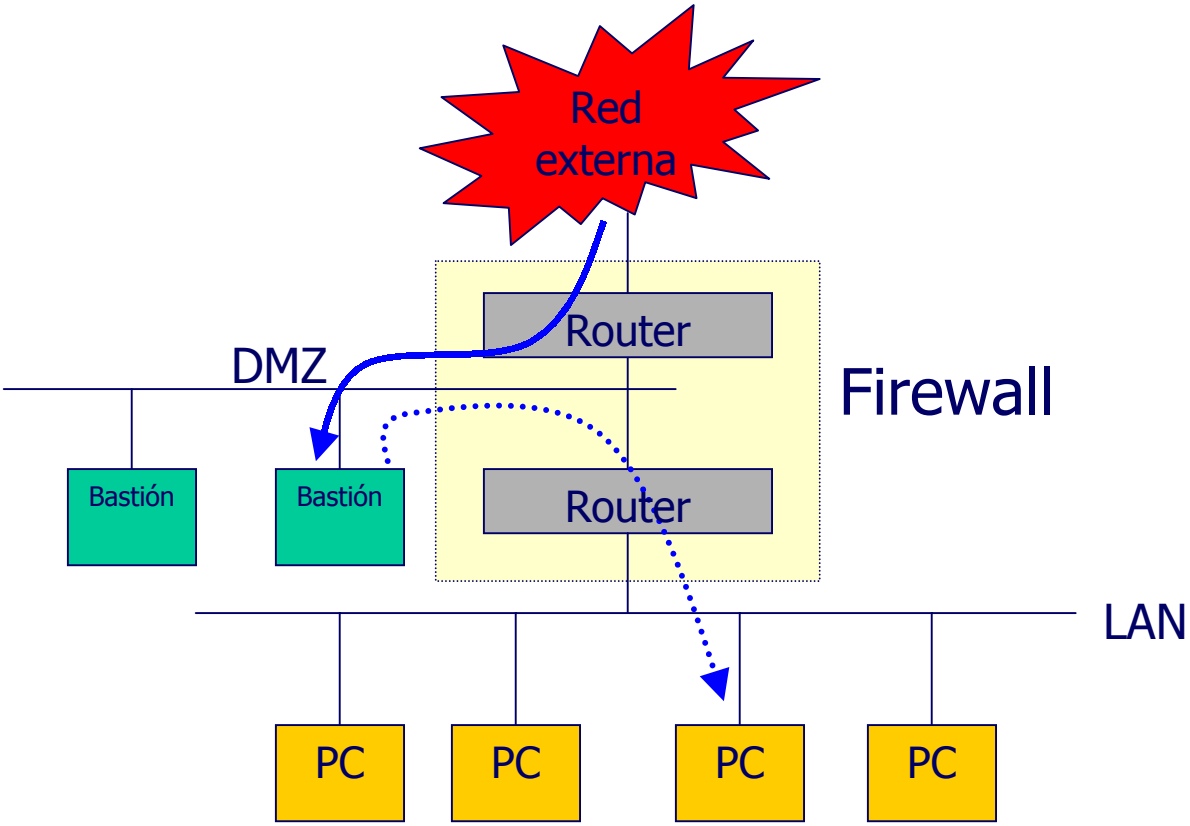


Arquitecturas de Firewalls

Las arquitecturas más sencillas se corresponden al esquema de "un router con filtros". En este caso, los paquetes entrantes deben pasar por un único equipo para pasar de Internet a la Red interna (LAN).
En esta arquitectura, los equipos que deben quedar expuestos a Internet (por ejemplo, servidores de correo, servidores HTTP, servidores FTP, etc) están en la LAN interna. Un atacante que tenga acceso a estos equipos, tendrá por tanto acceso a un equipo **dentro** de la LAN de la Empresa, y esto puede comprometer a la seguridad.



Una arquitectura más segura consiste en implementar, mediante dos "routers con filtros", una zona de seguridad intermedia, en la que se ubican todos los equipos que deben quedar expuestos en la red externa. Estos equipos "expuestos" a Internet, son llamados "Bastiones". Esta "zona intermedia" es conocida generalmente como "zona desmilitarizada", o DMZ (DeMilitarized Zone). Aunque un atacante que tenga acceso a estos equipos, no tendrá acceso directo a la LAN de la Empresa. Todavía tendrá que pasar por otro router con sus filtros, lo que brinda un nivel de seguridad adicional a la arquitectura anterior.
Muchos equipos "Firewall" implementan esta arquitectura, disponiendo de 3 puertas: una para la conexión a la red pública (Internet), otra para la DMZ y la última para la conexión a la LAN.



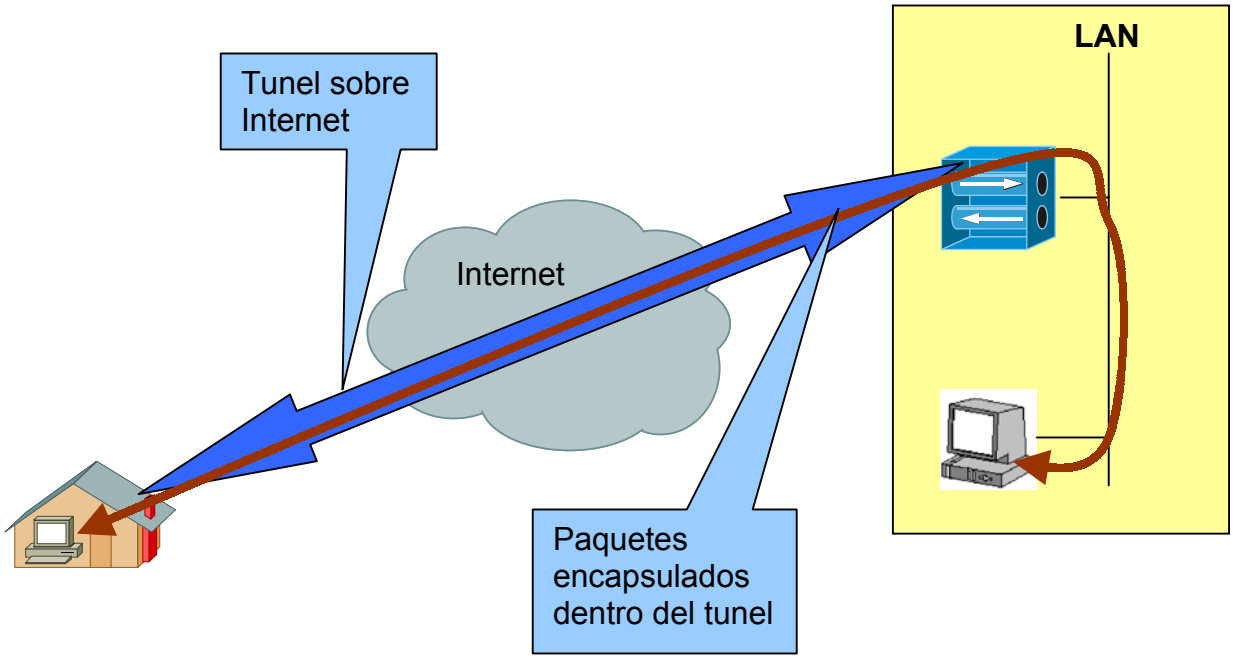
8.2.2 VPN

Una “Red Privada Virtual” o “Virtual Private Network” (VPN) [28] es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Las VPN permiten interconectar redes LAN a través de Internet, o computadores aislados a las redes LAN a través de Internet. Las VPN posibilitan la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo **túneles virtuales** entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

La tecnología de túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desencapsulado volviendo así a su estado original. En el traslado a través de Internet, generalmente los paquetes viajan encriptados, por razones obvias de seguridad.

En la LAN se debe ubicar un equipo “Terminador de túneles”, y los “clientes remotos” (PCs conectados a Internet que desean establecer un túnel con la LAN) deben tener el software adecuado para establecer túneles.



Una vez establecido el “túnel”, a nivel lógico, el PC remoto es como si estuviera en la LAN. Se le asigna una IP de LAN (generalmente con DHCP), y todos los servicios accesibles en la LAN están a disposición del PC remoto. Los paquetes IP que envía el PC remoto hacia la LAN son encapsulados, y generalmente encriptados, dentro del cuerpo del paquete IP que es enviado a Internet. El “Terminador de túneles”, ubicado en la empresa, recibe el paquete público, desencapsula y desencripta su contenido, y lo envía como un paquete IP normal de LAN

Hay varios sistemas de encriptación, pero el que está siendo más utilizado es el conocido como **IPSec**.

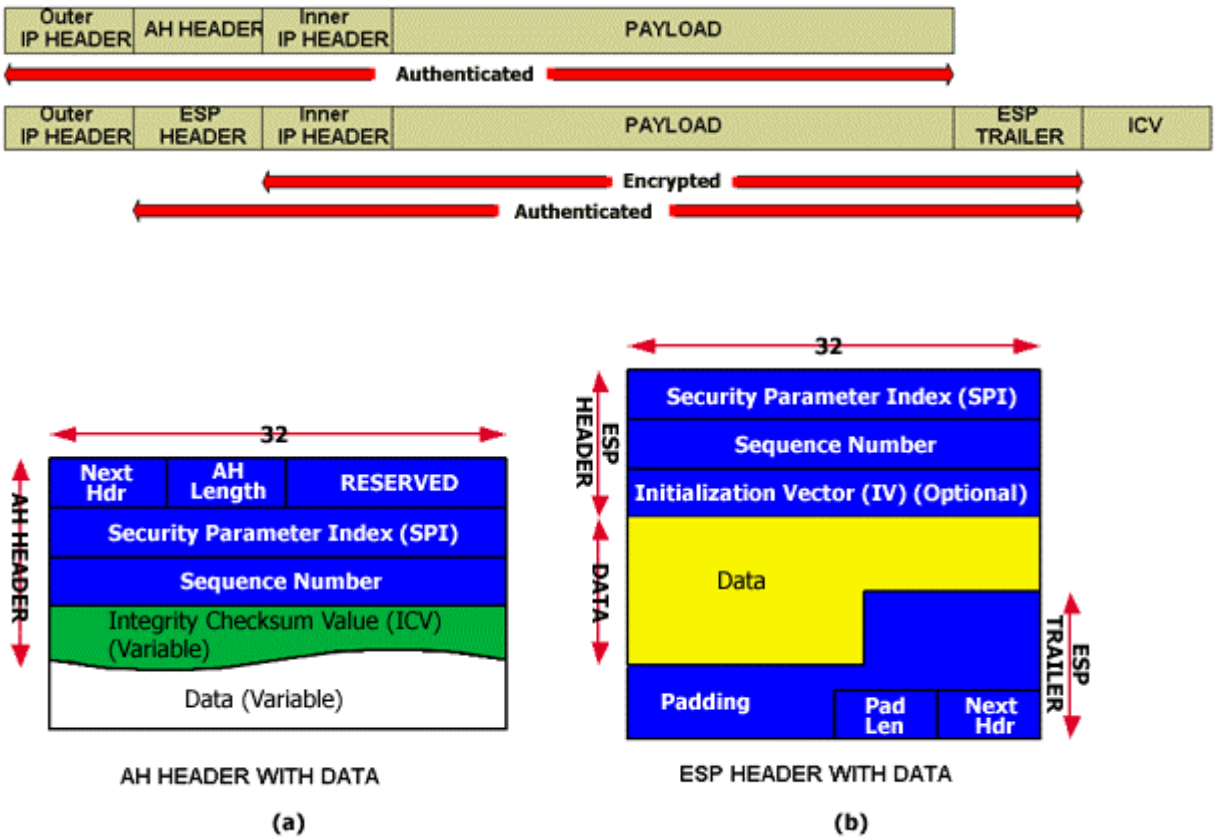
IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Se entiende por “confidencialidad” que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por “integridad” se entiende que los datos no sean modificados en el trayecto de la comunicación. “Autenticidad” indica sea confiable el remitente de los datos, y por “protección a repeticiones” se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

El protocolo AH [29] provee autenticación, integridad y protección a repeticiones pero no confidencialidad.

El protocolo ESP [30] provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

La siguiente figura muestra un paquete AH y un paquete ESP [31]. En el primero (AH), el cabezal AH (AH Header) incluye la autenticación de todo el paquete, incluyendo la dirección IP del comienzo del paquete. Es decir, el cabezal AH incluye un campo ICV (Integrity Checksum Value). En el segundo (ESP), la dirección IP del comienzo del paquete no tiene validación, pero el resto del paquete está encriptado y autenticado. EL ICV en este caso se encuentra al final del paquete



9 Referencias

1 “Redes de Computadoras”

Andrew S. Tanenbaum, Prentince Hall Hispanoamericana, 1997

2 “Breve Historia de las Telecomunicaciones”

José Joskowicz, Marzo 2004

3 “The Aloha System - Another Alternative for Computer Communications “

N. Abramson, Proceedings of Fall Joint Computer Conference, AFIPS Conference Proceedings, Vol. 37, pp. 281-285, 1970

4 IEEE 802.3-2002

IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

http://standards.ieee.org/getieee802/802.3.html

5 “Cableado Estructurado”

José Joskowicz, Junio 2003

6 IEEE 802.1d – Spannig Tree

IEEE Standard for Information technology--Telecommunications and information exchange between systems--IEEE standard for local and metropolitan area networks--Common specifications--Media access control (MAC) Bridges (includes IEEE 802.1k-1993), 1998 Edition or 2003 Edition

http://standards.ieee.org/getieee802/802.1.html

7 IEEE 802.1q – VLAN

IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks, 2003 Edition

http://standards.ieee.org/getieee802/802.1.html

8 IEEE 802.1p - Priorización

Traffic Class Expediting and Dynamic Multicast Filtering (published in 802.1D-1998)

9 IEEE 802.11 – Inalámbricos.

IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition

http://standards.ieee.org/getieee802/802.11.html

10 IEEE 802.11a :
Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band
(IEEE Standard for Information technology, 1999)

11 IEEE 802.11b :
Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
(IEEE Standard for Information technology, 1999)

12 IEEE 802.11g :
Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band
(IEEE Standard for Information technology, 2003)

13 “The Basic Guide to Frame Relay Networking”

Frame Relay Forum, 1998

14 xDSL Tutorial

Brandon Provolt
Engineering Intern Marketing and Product Development Group
Schott Corporation
Version 0.53 (beta), August 2000

15 ADSL
ITU-T Recomendación G992.1
(ITU-T, Jun 1999)

16 ADSL Light
ITU-T Recomendación G992.2
(ITU-T, Jun 1999)

17 HDSL
ITU-T Recomendación G991.1

(ITU-T, Oct 1998)

18 ANSI T1E1.4
High Bit Rate Digital Subscriber Line 2nd Generation (HDSL2)

19 ISO/IEC 7498-4 Information Processing Systems – Open Systems Interconnection – Basic Reference Model Part 4: Management Framework", 1989

20 Introduction to TMN
http://www.simpleweb.org/tutorials/tmn/index.html

Aiko Pras, Enschede, the Netherlands

Abril 1999

21 CCITT Blue Book "Recommendation M.30, Principles for a Telecommunication Management Network", Volume IV, Fascicle IV.1, Geneva, 1989

22 CCITT "Recommendation M.3010, Principles for a Telecommunication Management Network", Geneva, 1996

23 Nueva visión en la gestión de redes y servicios

José Antonio Lozano López, Carmen de Hita Álvarez

Telefónica I+D, Número 18, Setiembre 2000,

http://www.tid.es/presencia/publicaciones/comsid/esp/articulos/home.html

24 RFC-1098 SMNP, J. Case et al, MIT Laboratory for Computer Science, 1989

25 ISO/IEC 17799:2000: Information technology -- Code of practice for information security management

26 British Standards Institution. BS 7799-2:2002: Information security management systems - specification with guidance for use.
Londres, 2002

27 Internet Firewall Tutorial – A white paper

Rob Pickering
RPA Network, July 2002

28 Virtual Private Networks
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml
Mariano Hevia

29 RFC 2402 - IP Authentication Header
S.Kent BBN Corp, R. Atkinson @Home Network
November 1998

30 RFC 2406 - IP Encapsulating Security Payload (ESP)
S.Kent BBN Corp, R. Atkinson @Home Network
November 1998

31 IPSec VPN Fundamentals
Pradosh Kumar Mohapatra and Mohan Dattatreya
Tasman Networks, TechOnLine, Sep. 19, 2002