Capa de Red

La capa de red provee los medios para establecer, mantener y terminar conexiones de red entres sistemas abiertos comunicando entidades de aplicaciones y los medios funcionales para intercambiar unidades de datos de servicio de red entre entidades de transporte sobre conexiones de red.

Servicios: el servicio básico de la capa de red es proveer de transferencia transparente de datos entre entidades de transporte. Este servicio permite estructurar y detallar el contenido de datos para ser determinado exclusivamente por las capas superiores. Todos los servicios son provistos a un costo conocido.

- Direcciones de Red
- Conexiones de Red
- Transferencia de unidades de servicio de datos
- Calidad de los parámetros de servicios
- Notificación de errores
- Flow control
- Secuencionamiento
- Confirmación de recepción

Protocolos:

- X.25
- Internet Protocol (IP)
- Internetwork Packet Exchange (IPX)
- Datagram Delivery Protocol (DDP)
- Network Basic Input/Output System (NetBIOS)

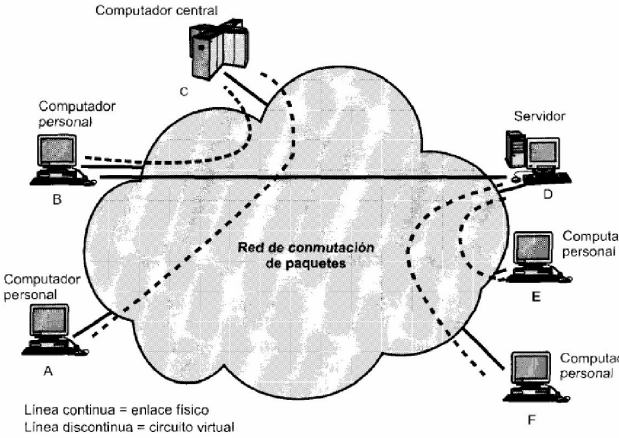
Funciones

- Ruteo
- Conexión de red
- Multiplexado
- Detección de errores

- Flow control
- Transferencia de datos
- Selección de servicios
- Gestión de la capa de red

Recomendación X.25

Es un protocolo estándar orientado a la conexión, que especifica una interfaz entre el equipo terminal de datos (DTE, Data Terminal Equipment) y el equipo de terminación de circuito de datos (DCE, Data Circuit-terminating Equipment) para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados.

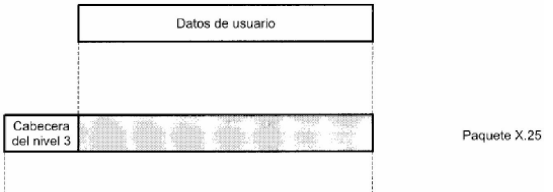


El estándar especifica 3 capas de protocolos: física, de enlace y de paquete. Estas 3 capas corresponden a las capas inferiores del modelo OSI.

X.25 hace uso de la especificación de la capa física dada en el estándar conocido como X.21 y para la capa de enlace se utiliza LAPB. El nivel de paquete proporciona un servicio de circuito virtual externo, lo que posibilita a un abonado de la red establecer conexiones lógicas, llamadas circuitos virtuales, con otros abonados.

El procedimiento balanceado de acceso al enlace (LAPB) es un subconjunto simplificado de HDLC que se usa únicamente para conectar una estación a una red. Por tanto, proporciona únicamente aquellas funciones básicas de control necesarias para la comunicación entre un DTE y un DCE. Por ejemplo, no incluye los caracteres de sondeo y de selección). LAPB se usa únicamente en las configuraciones balanceadas de dos dispositivos, donde ambos dispositivos son de tipo combinado. La comunicación se realiza siempre en modo balanceado asíncrono.

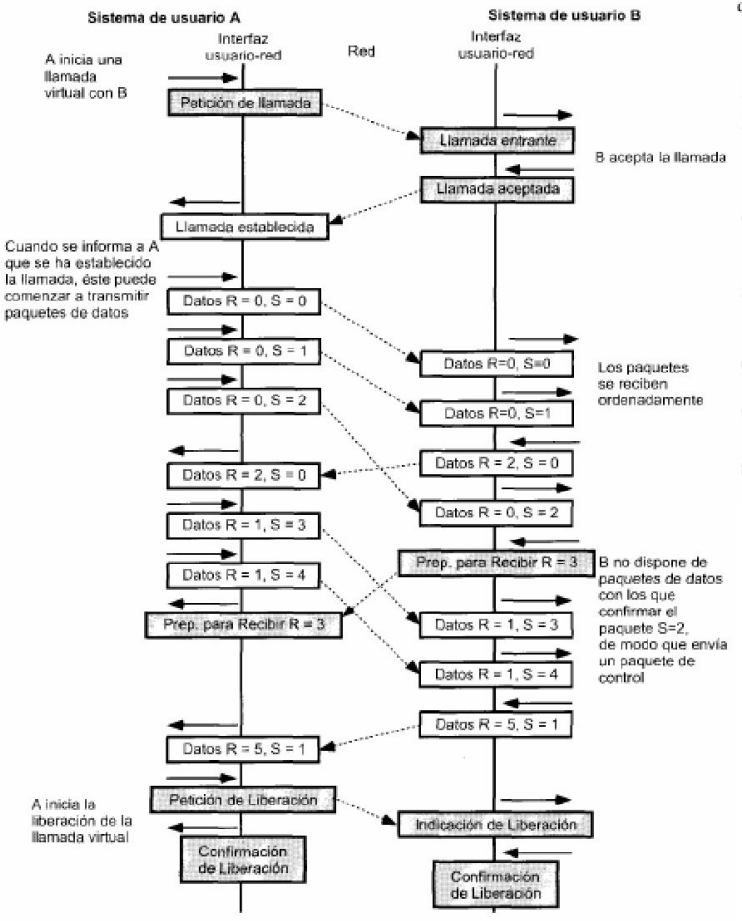
Los datos de usuario se pasan hacia abajo al nivel 3 de X.25, que les añade una cabecera consistente en información de control dando lugar a un paquete. Los datos de usuario se pueden segmentar en varios paquetes. La información de control incluida en el paquete tiene dos objetivos:



1) Identificación de un circuito virtual dado mediante un número al que se asociaran los datos.
2) Definición de números de secuencia para su uso en el control de flujo y de errores sobre los circuitos virtuales.

El paquete X.25 completo se pasa a la entidad LAPB, que añade información de control al principio y al final del paquete, dando lugar a parte de una trama LAPB. Es LAPB el que se encarga de que lleguen correctamente los paquetes X.25 que se transmiten a través de un canal susceptible de errores, desde o hacia la interfaz DTE/DCE. La diferencia entre paquete y trama es que los paquetes se crean en el nivel de red y se insertan dentro de una trama, la cual se crea en nivel de enlace.

Ofrece 2 tipos de circuitos virtuales, o **canales lógicos**: llamadas virtuales y circuitos permanentes. Una **llamada virtual,** o circuito conmutado, es un circuito virtual que se establece dinámicamente mediante una petición de llamada y una liberación de llamada. Un **circuito virtual permanente** es un circuito virtual fijo asignado en la red. La transferencia de los datos se produce como con las llamadas virtuales, pero en este caso no se necesita realizar ni el establecimiento ni el cierre de la llamada. En total, X.25 soporta 4096 canales lógicos distintos.



La secuencia de eventos es la que sigue:

1. A solicita un circuito virtual a B mediante el envío de un paquete Petición de Llamada («Call quest») al DCE de A. El paquete incluye las direcciones de origen y de destino así como el número a usar para este nuevo circuito virtual. Las futuras transmisiones de entrada y salida s identificarán mediante este número de circuito virtual.
2. La red encamina esta petición de llamada al DCE de B.
3. El DCE de B recibe el paquete Petición de Llamada y envía un paquete Llamada Entrante («In coming Call») a B. Este paquete tiene el mismo formato que el de Petición de Llamada, per con un número de circuito virtual diferente. Este número lo elige el DCE de B de entre el con junto de número locales libres.
4. B indica la aceptación de la llamada mediante el envío de un paquete Llamada Aceptada («Ca Accepted»), que especifica el mismo número de circuito virtual que el del paquete Llamada En trante.
5. El DCE de A recibe el paquete Llamada Aceptada y envía a A un paquete Llamada Establecid («Call Connected»). Este paquete tiene el mismo formato que el de Llamada Aceptada, pero e número de circuito virtual es el mismo que el del paquete Petición de Llamada original.
6. A y B se intercambian paquetes de datos y de control haciendo uso de sus respectivos número de circuito virtual.
7. A (o B) envía un paquete Petición de Liberación («Clear Request») para liberar el circuito vir tual y recibe un paquete Confirmación de Liberación («Clear Confirmation»).
8. B (o A) recibe un paquete Indicación de Liberación («Clear Indication») y transmite uno d Confirmación de Liberación («Clear Confirmation»).

FORMATO DE LLAMADA	
Identificador general del paquete	Grupo de canal logico
Numero de canal logico	
Identificador del tipo de paquete	
Longitud de la direccion que llama	Longitud de la direccion llamada
Direccion del que llama	
Direccion del llamado	
0 0	Longitud de las facilidades
Facilidades	
DATOS DEL USUARIO	

Formato del Paquete

Internet Protocol

Internet es una red global que proporciona un amplio rango de aplicaciones interpersonales y aplicaciones multimedia interactivas. Todas las redes de acceso disponen de una pasarela de acceso y la interred global está formada por un conjunto de redes regionales, nacionales e internacionales que se interconectan entre sí mediante líneas de alta velocidad y dispositivos denominados **pasarelas de conmutación** (switch) o simplemente **encaminadores** (routers).

En general, las distintas redes de acceso tienen asociados parámetros operacionales diferentes. Por lo tanto, es necesario que las operaciones de encaminamiento y retransmisión que realizan las pasarelas de acceso y los encaminadores se lleven a cabo a nivel de la capa de red. El más utilizado es el protocolo de

internet IP que, para poder transmitir paquetes de datos de un computador a otro, el protocolo IP debe estar presente tanto en los computadores terminales como en las pasarelas de acceso.

El protocolo IP de cada computador utiliza una dirección única de internet asignada a dicho equipo. Esta dirección se conoce como dirección de internet del computador o, más popularmente, dirección IP. Cada dirección IP está formada por dos campos: un **identificador/número de red o *netid*** y un **identificador/número de computador o *hostid.*** La asignación de identificadores de red se gestiona de forma centralizada desde una organización llamada **Compañía de internet para la asignación de nombre y numeración** (ICANN).

Cada uno de los routers construye una **tabla de encaminamiento** que le permite encaminar cualquier paquete/datagrama hacia cualquier otra red/netid que forme parte de Internet. De esta forma, cuando un encaminador recibe un paquete, simplemente lee el netid destino de la cabecera y utiliza los contenidos de su tabla de encaminamiento para reenviar el paquete por el camino/ruta adecuado, para que el paquete llegue primero hasta el router de interred asociado al destino y después desde este hasta la pasarela de acceso de la red destino. El protocolo IP del computador destinatario elimina la cabecera del paquete y pasa el bloque de información que contiene datos o carga útil al protocolo de la capa de transporte indicando la cabecera del paquete.

Si el tamaño del paquete es mayor que el tamaño máximo de trama, es decir, la unidad máxima de transmisión (MTU) de la red de acceso destinataria, el protocolo IP de la pasarela de acceso destinatario procederá a dividir el bloque de datos contenido en el paquete en bloques de menor tamaño conocidos como fragmentos. Después, cada fragmento se reenvía hacia el computador destinatario en un paquete individual cuya longitud viene determinada por la MTU de la red de acceso. El destinatario debe reensamblar los fragmentos de datos recibidos en estos paquetes para formar el bloque original de datos.

En la práctica, para realizar las distintas funciones, se utilizan diferentes protocolos adjuntos como:

- **Protocolo de resolución de direcciones (ARP)** que se utiliza en el caso de computadores conectados a una LAN de difusión para determinar la dirección física MAC asociada a un computador o pasársela a partir de su dirección IP.
- **Protocolo de mensajes de control de internet (ICMP)** que es utilizado por un computador o pasarela para intercambiar mensajes de error y otros mensajes de control con otro computador.

Datagrama o Paquete IPv4

IP es un protocolo sin conexión y todos los datos de usuario se transmiten en el campo de datos o carga útil del paquete o datagrama.

Versión contiene la versión del protocolo IP que se utilizó para construir el paquete.

IHL especifica la longitud real de la cabecera expresada en múltiplos de palabras de 32 bits. La longitud mínima de la cabecera es de 5 palabras.

TOS (Type of Service) permite a los procesos o protocolos de aplicación especificar la prioridad relativa de los datos. Las distintas pasarelas y encaminadores utilizan este campo para transmitir primero los paquetes de mayor prioridad.

Longitud Total define la longitud total del diagrama inicial, incluyendo la parte de cabecera y de carga útil (datos). Si el contenido del datagrama inicial tiene que dividirse en varios paquetes de menor tamaño (fragmentos), el destinatario utilizara el valor de longitud total para reensamblar los datos contenidos.

Los 3 campos siguientes son tres bits, de los cuales se utilizan los dos últimos:

- **Indicador de no fragmentar o bit D**. La activación de este bit se realiza en el computador fuente y cualquier encaminador puede examinar su valor. Un 1 indica que o bien el paquete se transfiere íntegramente o, de otro modo, no debe transferirse.
- **Indicador de más fragmentos o bit M**. Se utiliza en el proceso de reensamblaje, en este caso tiene valor 1 en todos los paquetes o fragmentos excepto en el último, cuyo bit M tiene valor 0.

Desplazamiento de Fragmento se utiliza en el procedimiento de reensamblaje para indicar la posición que ocupa el primer byte de los datos contenidos en el fragmento con relación al bloque completo de datos del paquete original.

Tiempo de Vida define la cantidad de tiempo máximo que puede permanecer el paquete en tránsito a través de internet. Cada pasarela o encaminador va restando a este valor una cantidad específica y, en caso de que su valor llegue a cero, el paquete debe ser descartado.

Protocolo permite que el protocolo IP destinatario pueda asar los datos de cada paquete recibido al mismo protocolo que envió los datos.

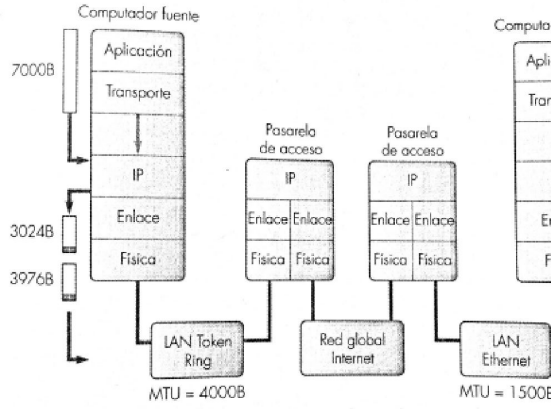
Suma de comprobación de la cabecera o Redundancia se aplica sobre la cabecera del datagrama y se utiliza como salvaguarda contra el encaminamiento de paquetes erróneos hacia destinos incorrectos.

Las direcciones fuente y destino son las direcciones IP a nivel de internet de los computadores fuente y destino respectivamente.

Opciones se utiliza en algunos datagramas seleccionados para transportar información adicional relacionada con: *seguridad, encaminamiento de origen, encaminamiento de origen flexible, registro de ruta, identificador de secuencia, sello de tiempo.*

Fragmentación y Reensamblado

Si el tamaño del paquete es mayor que la MTU de la red de acceso destinataria o de un encaminador intermedio, tendrá que dividir los datos contenidos en el paquete en un determinado número de bloques de menor tamaño denominados fragmentos. El destinatario debe reensamblar los fragmentos de datos contenidos en cada uno de los paquetes recibidos y formar el bloque de datos original.



A modo de ejemplo, supongamos que el protocolo de transporte de un computador conectado a una red de tipo *token ring* transfiere un bloque de 7000 bytes, incluyendo la cabecera del protocolo de transporte, a través de internet a otra computadora conectada a una red Ethernet. Supongamos que la MTU asociada a la red token ring es de 4000 bytes, que la MTU de la red es de 1500 bytes y que la cabecera de cada datagrama IP es de 20 bytes.

Debido a que la cabecera de cada datagrama ocupa 20 bytes, la cantidad máxima de datos que pueden contener una trama de la red token ring es 4000-20=3980. De la misma forma, la cantidad máxima de datos que puede contener una trama de la red Ethernet es 1500-20=1480 bytes. El número de bytes de datos de todos los fragmentos debe ser múltiplo de 8, por lo tanto, es necesario limitar la cantidad de datos de usuario en cada paquete de la red token ring a un máximo de 3976 bytes. En el caso de Ethernet, 1480 es divisible por 8, por lo tanto, es un valor válido.

Para transferir el bloque de 7000 bytes a través de la red, es necesario dividirlo en dos datagramas, el primero contendrá 3976 bytes de datos y el segundo 7000-3976=3024 bytes. Puesto que el valor máximo de datos en la red LAN ethernet destinataria es sólo 1480 bytes, será necesario volver a fragmentar ambos paquetes.

El primer datagrama se fragmenta en dos paquetes de tamaño máximo (1480 bytes) y un tercer paquete de 3976-2x1480=1016 bytes. El segundo datagrama se fragmenta también en dos paquetes de tamaño máximo (1480 bytes) y un último paquete de 3024-2x1480=64 bytes. Cuando los paquetes alcanzan su

destino, el protocolo IP del computador receptor reensambla los seis fragmentos recibidos para formar el bloque de información de 7000 bytes original.

El procedimiento de fragmentación puede parecer sencillo, pero presenta algunos inconvenientes. Si después de enviar un bloque no se recibe una confirmación de la recepción del mismo dentro de un intervalo de tiempo máximo establecido, la fuente deberá retransmitir el bloque completo. En el ejemplo anterior, en caso que tan solo uno de los seis fragmentos se retrase o sea descartado, provocará la retransmisión del bloque completo de 7000 bytes.

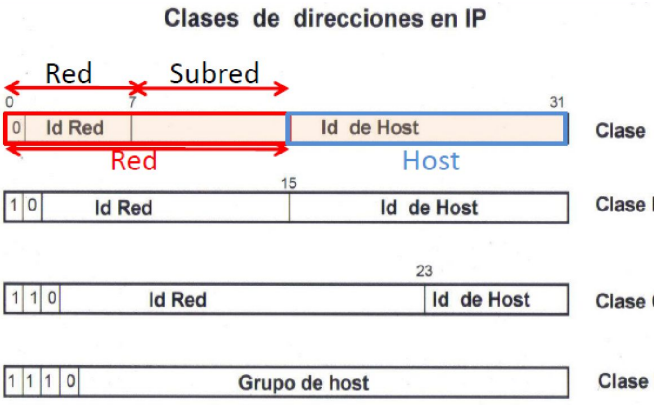
Para solucionar este problema, existe la posibilidad que el protocolo IP fuente, antes de enviar cualquier dato procedente del protocolo de transporte, determine la MTU de la ruta que debe seguir el paquete a través de internet. Entonces, si la MTU de la ruta es menor que los datos de usuario, el protocolo fuente fragmentara estos datos usando dicha MTU. De esta manera, los datos podrán viajar a través de la interred global sin necesidad de volver a sufrir nuevas fragmentaciones.

Direcciones IP

Cada computador, pasarela o encaminador tiene asignada una única dirección IP a nivel de internet, que está formada por una parte de identificador de red (ID Red) y otra parte de identificador de computador (ID Host). De esta forma, el ID de Red identifica a la red que está conectado un computador y el ID Host identifica al computador concreto dentro de la red.

Direcciones basadas en clases

Para disponer de una cierta flexibilidad a la hora de asignar ID de Red, el esquema de direccionamiento consiste en dividir el espacio de direcciones de 32 bits en cinco formatos diferentes de direcciones. Las clases A, B, y C se utilizan para representar direcciones individuales, es decir, para comunicaciones entre parejas de computadoras.



La clase concreta a la que pertenece una dirección puede determinarse por la posición del primer bit con valor cero dentro de los cuatro primeros bits. El resto de los bits se utilizan para especificar la parte del ID de Red y la parte del ID del Host.

Las direcciones de clase A están pensadas para redes que contienen un gran número de computadores (hasta 2^24), mientras que las direcciones de clase C permiten disponer de un gran número de redes, cada una de ellas con un pequeño número de computadores (hasta 256). Un ejemplo de red de clase A podría ser una gran red nacional y un ejemplo de red de clase C una pequeña LAN de una organización.

Los ID Host y Red que tengan todos los bits en 0 todos los bits en 1 tienen un significado especial:

- Una dirección con todos los bits del ID Host en 0 hace referencia a la red especificada en el ID de Red en lugar de hacer referencia a un computador.
- Una dirección con todos los bits a 1 se utiliza para enviar un paquete de difusión a la red fuente.
- Una dirección con todos los bits del ID Host a 1 se utiliza para enviar un paquete de difusión a la red destino especificada en el ID de Red de la dirección destino.
- Una dirección de clase A con todos los bits del ID de Red en 1 se utiliza para la realización de comprobaciones de la arquitectura de protocolos del computador fuente. Esta dirección se conoce como **dirección de bucle local**.

Para facilitar la utilización de direcciones IP, los 32 bits de la dirección se dividen en cuatro bytes. Cada byte se convierte a su valor decimal equivalente, de manera que la dirección IP se representa mediante los cuatro números decimales separados entre sí por puntos. Esta forma de representación se denomina notación de punto. Ejemplo:

00001010 00000000 00000000 00000000 = 10.0.0.0

Subredes

El concepto de subredes fue introducido para separar los encaminadores asociados a una organización particular de las funciones de encaminamiento en la interred global. La idea fundamental consiste en que, en lugar de que cada LAN dentro de la organización tenga su propio ID de Red, se utiliza un único ID de Red para toda la organización. Cada LAN dentro de la red de la organización se conoce como una subred y la identidad de cada subred (LAN) forma parte del campo Host ID.

Cuando se usan subredes, se utilizan las mismas clases y estructuras de direcciones, con la diferencia de que el ID de Red identifica a una organización completan en lugar de una subred individual. De esta forma, el ID de Red se considera como el identificador de la parte de internet. El Host ID está formada por dos subcampos: una parte de identificador de subred y otra parte de Host ID local.

Debido al amplio rango posible de subredes, en cada red concreta (con un ID de Red determinado) se utiliza una **máscara de subred** para definir los límites entre la parte de subred y la parte del Host ID local. La máscara de dirección se guarda en la pasarela de la organización y en todos los encaminadores entre subredes dentro de la organización. Está formada por un conjunto de bits a 1 en las posiciones que se corresponden con la dirección de red (ID de Red y el ID de Subred) y un conjunto de bits a 0 en las posiciones que se corresponden con el Host ID. Por ejemplo:

11111111 11111111 11111111 00000000 = 255.255.255.0

Significa que los tres primeros bytes contienen el identificador de red/subred (ID de Red/ ID de Subred) y el cuarto byte contiene el identificador del computador (Host ID)

ARP (Adress resolution protocol)

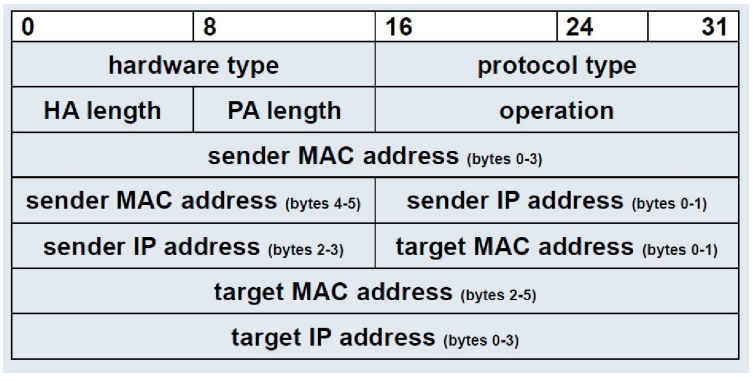
Este protocolo se utiliza para averiguar la dirección MAC a partir de la dirección IP del computador o pasarela conectado a la misma LAN.

Un computador puede tener asociado dos direcciones: la IP y la dirección MAC. La dirección MAC se asigna durante el proceso de fabricación, se conoce también como dirección de hardware o física. Ambas direcciones (IP y MAC) se almacenan en un archivo de configuración en el disco duro del computador.

El protocolo ARP tiene asociada una tabla de encaminamiento conocida como cache ARP. Esta cache contiene una lista de las parejas de direcciones IP/MAC de todos los computadores con los que se ha comunicado recientemente, si el computador esta recién conectado, esta tabla estará vacía.

Al recibir el datagrama procedente del protocolo IP del computador A, el protocolo ARP de A lee la dirección IP destino B contenida en la cabecera del datagrama y comprueba que esta dirección no está en la cache. Entonces el protocolo ARP de A envía un mensaje de solicitud ARP en una trama de difusión a la LAN y espera recibir una respuesta. El mensaje de solicitud contiene la pareja de direcciones IP/MAC del computador A y la dirección IP del computador B.

El protocolo ARP del computador B reconoce su propia dirección IP en el mensaje de solicitud y procede a procesar dicho mensaje. Primero comprueba si la pareja de direcciones fuente están almacenadas en su cache ARP, si no están, entonces las guarda en la tabla. A continuación, el protocolo ARP del computador B devuelve su propia dirección MAC mediante un mensaje de respuesta ARP al computador A, usando como dirección destino la dirección MAC de A. A recibe el mensaje de respuesta, introduce la pareja de direcciones IP/MAC de B en su cache.



Para enviar un datagrama, por ejemplo, desde el computador A, hasta un computador en una LAN diferente el protocolo ARP de A envía un mensaje ARP de la misma forma que en el caso anterior. Cuando la pasarela recibe este mensaje y determina que la

parte de ID de Red de la dirección IP destino pertenece a una red diferente, entonces responde mediante un mensaje ARP de respuesta que contiene la pareja de direcciones IP/MAC de la propia pasarela. Entonces, el computador A añade esta entrada a su cache ARP y reenvía el datagrama hacia la pasarela como si esta fuese el computador destinatario. El protocolo IP de la pasarela se denomina **proxy ARP**.

Internet Control Message Protocol (ICMP)

El protocolo de mensajes de control de Internet se utiliza en computadores, encaminadores y pasarelas para llevar a cabo distintas funciones y especialmente para gestión de la red. Las funciones asociadas a ICMP son:

- Informe de errores
- Comprobación de equipo alcanzable
- Control de congestión
- Notificación de cambio de ruta
- Medición de rendimiento
- Direccionamiento de subredes

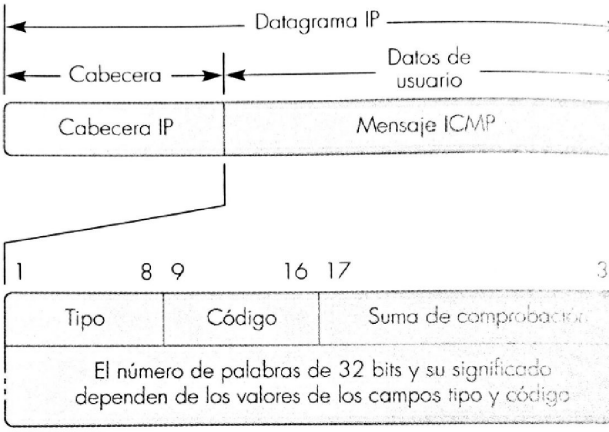
Los paquetes pueden ser descartados en su recorrido a través de internet. Aunque los errores de transmisión son un posible motivo de descarte, sin embargo, existe una gran variedad de razonas que pueden conducir a un computador, encaminador o pasarela a descartar un paquete. Si no existiese ningún mecanismo de informe de errores, un computador no tendría forma de saber si los fallos reiterados en el intento de transmisión de un paquete a un determinado destino son debidos a una calidad pobre de la línea de transmisión o simplemente a que el computador destinatario está apagado.

Cuando un paquete sufre errores de transmisión, sencillamente se descarta. Si un paquete se descarta por cualquier otra razón, el protocolo ICMPL genera un mensaje de informe de error de tipo *destino inalcanzable* y lo devuelve al protocolo ICMP del computador fuente indicando un código que indica la razón de descarte.

En general, la transferencia de un mensaje a través de la interred global es mucho más rápida cuando no se utiliza fragmentación La mayoría de las redes admiten una MTU (máxima frecuencia de transmisión). Una de las técnicas para garantizar que no se produce fragmentación, consiste en que el protocolo IP fuente utilice esa cantidad como tamaño máximo para todos los datagramas.

Una alternativa consiste en utilizar un procedimiento conocido como descubrimiento de la MTU del camino, que permite al protocolo OP fuente determinar la MTU del camino/ruta antes de enviar cualquier datagrama. Cuando se recibe el primer mensaje del protocolo de transporte relacionado con una nueva sesión/llamada, este se envía en un único datagrama con el bit de no fragmentar activado. Si algún encaminador dentro del camino no puede reenviar el paquete devolverá un informe de errores ICMP incluyendo el tamaño de la MTU que si es posible. El protocolo IP fuente adopta este tamaño como su propia MTU para enviar el resto de mensajes relacionados con la sesión/llamada.

Otra función de este protocolo es cuando un administrador de una red recibe la notificación de un usuario indicando que un destino específico no responde, puede averiguar el motivo usando la función de comprobación de alcance de equipo, que se implementa mediante un programa denominado **ping**. El administrador envía un mensaje de solicitud de eco al computador sospechoso para determinar si este esta encendido y si responde a los mensajes. Cuando se recibe un mensaje de solicitud de eco, el protocolo ICMP del destinatario lo transforma en un mensaje de respuesta de eco y lo devuelve.



Si un paquete se descarta porque el receptor no dispone de buffers de memoria libres debido a una situación de sobrecarga temporal, se devuelve un mensaje de enfriamiento de fuente al protocolo ICMP del computador fuente. Con este mensaje se solicita al computador fuente que reduzca el ritmo de envió de paquetes. Cada vez que se descarta un paquete se devuelve un

nuevo mensaje de enfriamiento de fuente, por tanto, el computador fuente va reduciendo de forma incremental el ritmo de envío.

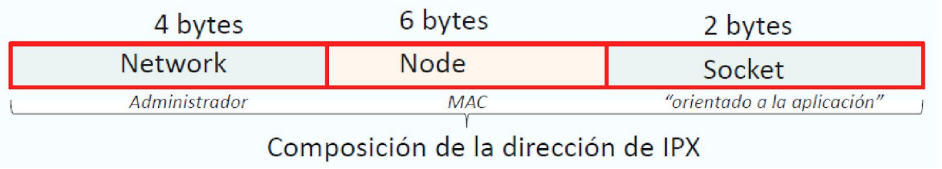
InternetworkPacketExchange IPX

Es un protocolo creado por Novell que interconecta redes que usan clientes y servidores Novell Netware. Está orientado a paquetes y no orientado a conexión (no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino).

Es un protocolo de datagramas y no fiable debido a que transmite datos a un nodo remoto, pero al no esperar una respuesta o una confirmación indicando si los datos han sido recibidos con éxito, no garantiza la entrega de datos. El término “datagrama”, significa que cada paquete se trata como una entidad individual, sin considerar ninguna relación lógica o secuencial con cualquier otro paquete.

IPX utiliza un esquema de direccionamiento de 12 bytes para transmitir sus paquetes de datos. La dirección de 12 bytes se divide en tres secciones:

- Redes de origen y destino, utilizadas para direccionar grupos de trabajo. Cada dirección de red tiene que ser única en la red (IPX/SPX).
- Nodos origen y destino. Direccionan nodos de red dentro de los grupos de trabajo (análogos a las direcciones de los adaptadores token-ring).
- Sockets origen y destino, se pueden utilizar para multiplexar funcione dentro de un nodo de red. Los sockets IPX permiten que varios protocolos de alto nivel utilicen los servicios IPX de forma concurrente.



Composición de la dirección de IPX

NetBIOS

NetBIOS, Sistema de Entrada Salida Básica de Red es un protocolo estándar de IBM, que permite que las aplicaciones sobre diferentes computadoras se comuniquen dentro de una red de área local (LAN). A su vez, provee los servicios de sesión descriptos en la capa 5 del modelo OSI. Es un protocolo de aplicación para compartir recursos en red. Se encarga de establecer la sesión y mantener las conexiones.

Pero este protocolo debe transportarse entre máquinas a través de otros protocolos; debido a que por sí mismo no es suficiente para transportar los datos en redes LAN como WAN, para lo cual debe usar otro mecanismo de transporte (Ej: en redes LAN protocolo NetBEUI, en redes WAN protocolo TCP/IP).

Es buena para redes semillas-semillas locales, pero no puede ser utilizada para trabajos de internet debido a que no netBEUI no soporta routeo, es decir, conexión a grandes redes.

Access Control List ACL

Una Lista de Control de Acceso es una lista de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Cada vez que se envía o se recibe un paquete, el router lo analiza comparándolo con la ACL correspondiente, línea por línea. Si encuentra una coincidencia, toma la acción correspondiente (aceptar o rechazar), y ya no revisa los restantes renglones. Es por eso que hay que listar los comandos desde los casos más específicos, hasta los más generales. Las excepciones tienen que estar antes de la regla general. Si no encuentra una coincidencia en ninguno de los renglones, rechaza automáticamente el tráfico. Considere que hay un "deny any" implícito, al final de cada ACL. Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.

Las ACL estándar (1-99) sólo permiten controlar en base a la dirección de origen. Las ACL extendidas (100-199) permiten controlar el tráfico en base a la dirección de origen; la dirección de destino; y el protocolo utilizado. Si consideramos sólo el tráfico de tipo TCP/IP, para cada interface puede haber sólo una ACL para tráfico entrante, y una ACL para tráfico saliente.

Las ACL no actúan sobre paquetes que se originan en el mismo router. Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.

- **ACL inbound** (de entrada): los paquetes entrantes se procesan antes de ser enrutados a la interfaz de salida.
- **ACL outbound** (de salida): los paquetes entrantes se enrutan a la interfaz de salida y luego son procesados a través de la ACL de salida.

Routing

Un **router** es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra. Todos los routers guardan una tabla de enrutamiento. Existe un proceso, denominado daemon de enrutamiento, que actualiza la tabla con todas las rutas conocidas. El núcleo del sistema lee la tabla de enrutamiento antes de reenviar paquetes a la red local. Una tabla de enrutamiento es un documento electrónico que almacena las rutas a los diferentes nodos en una red informática.

La información de enrutamiento que el router aprende desde sus fuentes de enrutamiento se coloca en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del router acerca de las redes. Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar los paquetes. Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se puede determinar de forma manual por el administrador de la red, dando lugar a rutas estáticas, o pueden ser definidas a través de procesos dinámicos que se ejecutan en la red, dando lugar al enrutamiento dinámico.

Las **tablas de enrutamiento estáticas** se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso de enrutamiento según los parámetros del administrador. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

Una **tabla de enrutamiento dinámica** se actualiza de forma periódica utilizando un protocolo de encaminamiento dinámico, como lo puede ser, RIP, OSPF o BGP. Cuando se produce algún cambio en la red, los routers deben actualizar sus tablas de enrutamiento con el fin de conseguir una entrega eficiente de los paquetes IP.

Protocolos de Enrutamiento

Los protocolos de encaminamiento son un conjunto de reglas y procedimientos que permiten formar las tablas de enrutamiento dinámicas, con el fin de realizar el paso de paquetes IP por el router en cuestión.

Un router recibe un paquete y lo reenvía a otra red. El problema está en saber por cuál de todos los caminos posibles que tiene cargado en la tabla de enrutamiento es el mejor y más eficiente para alcanzar ese punto. La solución a esto radica en la utilización de **métricas**. Una métrica es un costo que se le asigna al salto de una red a otra, por lo que se buscará que ese costo sea el menor posible. La selección de qué métrica utilizar depende del protocolo seleccionado.

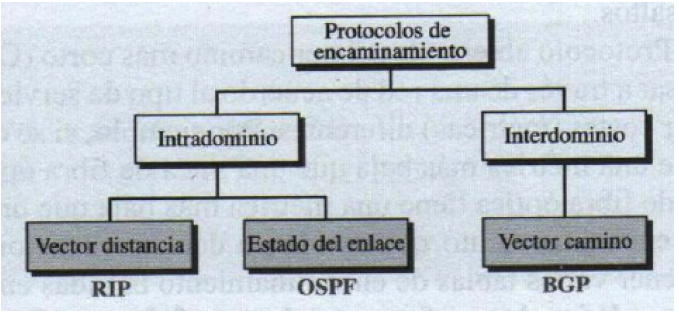
Enrutamiento interdominio e intradominio

Hoy en día, una red puede ser tan amplia, que un único protocolo puede ser incapaz de gestionar la tarea de actualizar las tablas de enrutamiento de todos los routers. Por esto, es que se divide las redes en sistemas autónomos. Un **sistema autónomo** es un grupo de redes y routers bajo la autoridad de una única

administración. El encaminamiento dentro de un mismo sistema autónomo se conoce como **enrutamiento intradominio**. En cambio, cuando el encaminamiento se da entre distintos sistemas autónomos, se conoce como **enrutamiento intradominio.**

Existen varios protocolos de enrutamiento interdominio, como intradominio, y un router puede tener tantos como el fabricante desee. El contar con más de un protocolo, hace posible que el mismo router pueda intercomunicarse con distintos sistemas autónomos. Será el router quien decida que protocolo utilizar frente a determinado sistema, y eso queda definido a partir de la definición de prioridades.

Los protocolos más utilizados son el Protocolo de Información de Encaminamiento RIP, implementado usando la métrica del vector distancia; el Protocolo Abierto del Primer Camino Más Corto OSPF, basado en el estado del enlace; y el Protocolo de Pasarela Frontera BGP, implementado usando vector camino. Los dos primeros protocolos, RIP y OSPF son protocolos interdominio, y el ultimo, BGP, es un protocolo intradomino.



Routing Information Protocol RIP

El enrutamiento de un protocolo basado en vector de distancias requiere que un router informe a sus vecinos de los cambios en la topología periódicamente y en algunos casos cuando se detecta un cambio en la topología de la red.

El **algoritmo vector distancia** se basa en calcular la dirección y la distancia hasta cualquier enlace en la red. El costo de alcanzar un destino se lleva a cabo usando cálculos matemáticos como la métrica del camino.

Los cambios son detectados periódicamente ya que la tabla de enrutamiento de cada router se envía a todos los vecinos que usan el mismo protocolo. Una vez que el router tiene toda la información, actualiza su tabla e informa a sus vecinos de los mismos.

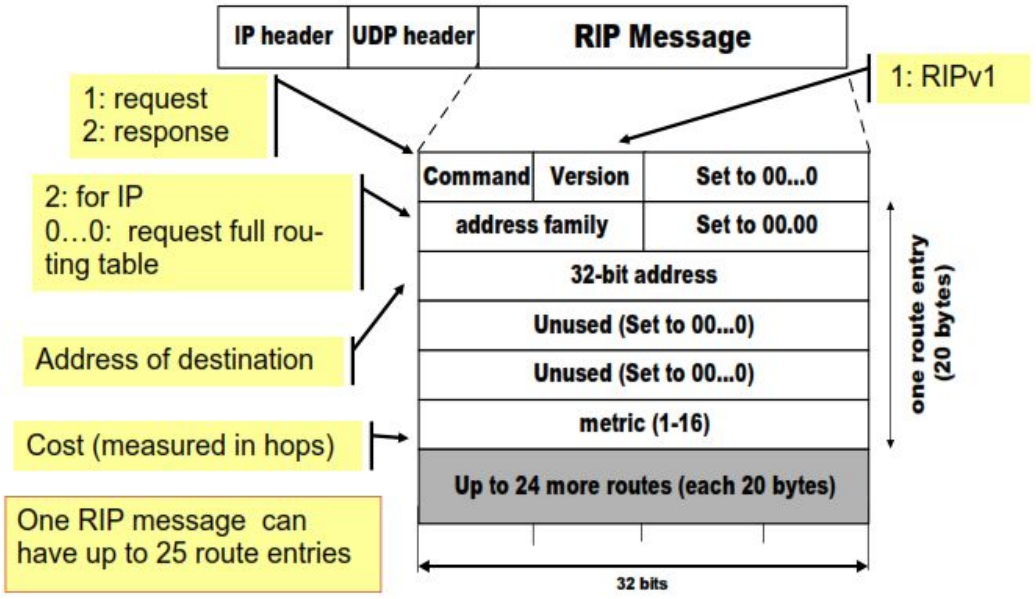
El algoritmo de vector distancia se adapta perfectamente al modo de aprendizaje de los nodos que "nacen", es decir, cuando se conectan a la red. A medida que el algoritmo progresa, el nuevo nodo va adquiriendo más información sobre el resto de nodos de la red. Este algoritmo converge rápidamente cuando se conectan nuevos nodos.

El P**rotocolo de Informacion de Encaminamiento** (Routing Information Protocol – RIP) es un protocolo de encaminamiento intradominio. Es el protocolo más sencillo y se basa en la utilización de un vector distancia. RIP utiliza la métrica **contador de saltos**, que define la cantidad de enlaces entre redes que se necesitan para alcanzar el destino. La máxima cantidad de saltos posibles que se pueden dar es 16, por lo que cualquier camino en un sistema autónomo que utilice RIP no puede superar los 15 saltos. Al llegar al salto 16, se considera como ruta inaccesible, o inalcanzable.

La actualización de las tablas de enrutamiento en el protocolo RIP se produce cada 30 segundos, es decir, que si se tiene 7 nodos, desde el Nodo1 al Nodo7, el Nodo2 será visible para el Nodo1 al cabo de los primeros 30 segundos. El Nodo3 empezará a formar parte de la tabla de enrutamiento recién al minuto de comenzado el protocolo. Esto implica, que al haber un máximo de 16 saltos, el Nodo1 recien podrá acceder al Nodo16 al cabo de 8 minutos.

La definición original, recogida en el RFC 1058, define RIP como un protocolo de enrutamiento con clase, es decir, basado en los tipos de máscaras de las direcciones IP. Por tanto, RIPv1 no soporta máscaras de tamaño variable ni direccionamiento sin clase. Esto implica que las redes tratadas por este protocolo deben tener la máscara de red predefinida para su clase de dirección IP, lo que resulta poco eficiente a la hora que existan subredes. Además, RIPv1 tampoco incluye ningún mecanismo de autentificación de los mensajes, haciéndolo vulnerable a ataques.

Debido a las limitaciones de la versión 1, se desarrolla RIPv2 en 1993, y se estandariza finalmente en 1998. Esta versión soporta subredes y se mantuvo la limitación de 15 saltos, con el fin de garantizar la retrocompatibilidad con RIPv1. RIPv2 soporta autenticación, utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, y autentificación mediante contraseña codificada mediante MD5.



Open Shortest Path First OSPF

Este protocolo se basa en el algoritmo de enrutamiento denominado **estado del enlace.** Este algoritmo de encaminamiento se basa en que cada nodo llegue a conocer la topología de la red y los retardos asociados a los enlaces, para que a partir de estos datos, pueda obtener el árbol y la tabla de encaminamiento tras aplicar el algoritmo de coste mínimo (algoritmo de Dijkstra) al grafo de la red. Esto implica que un router o encaminador entabla la comunicación entre un nodo, y todos los demás de la red, identifica cuáles son sus vecinos y a qué distancia está de ellos. Con la información que un nodo de la red recibe de todos los demás, puede construir un "mapa" de la red y sobre él calcular los caminos óptimos.

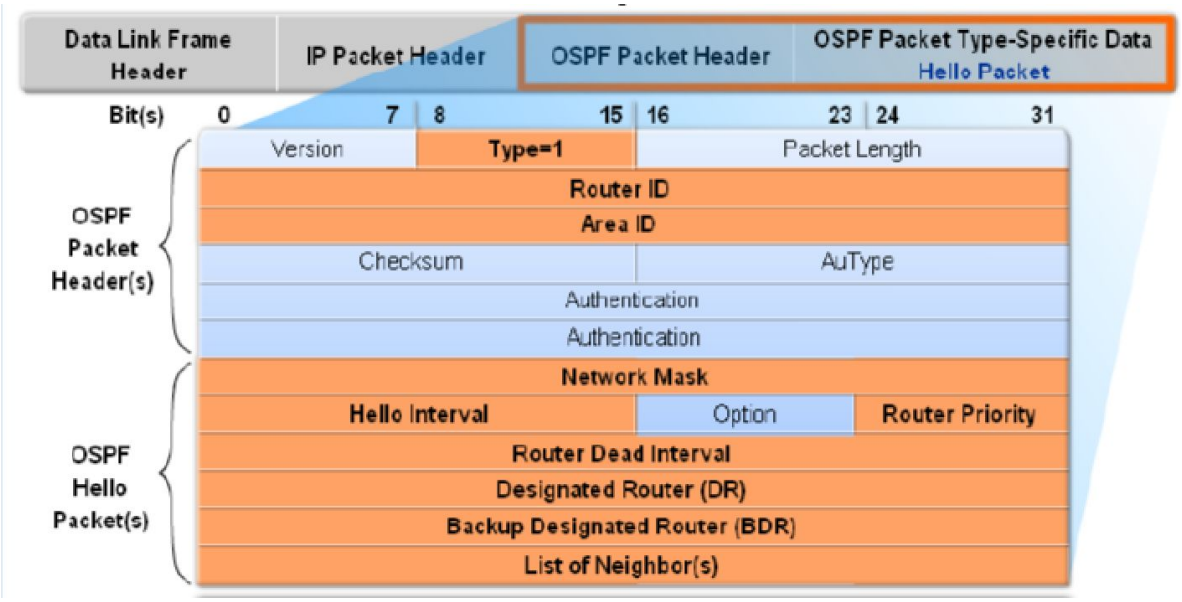
El cálculo de los costos mínimo para los caminos óptimos depende de la métrica que se quiera utilizar. El protocolo de estado del enlace soporta como métricas el retardo que existe entre un nodo y el otro, la velocidad soportada por el canal de transmisión que enlaza los nodos, o la mínima tasa de errores, buscando con este último, el camino que mejor porcentaje de fidelidad tenga.

El protocolo OSPF, **Protocolo Abierto de Primer Camino Más Corto**, es un protocolo intradominio basado en el enrutamiento de estado del enlace. Ademas de las métricas propias del algoritmo de enrutamiento utilizado, OSPF construye una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

Para tratar el encaminamiento de forma eficiente, OSPF divide el sistema autónomo en distintas áreas. Un **área** es una colección de redes, estaciones y routers conectados entre sí. Los routers en OSPF se dividen en dos tipos, routers internos, y de frontera de área. Los **routers internos** transmiten, dentro de cada área, información de encaminamiento. A su vez, los **routers de frontera de área** son los que resumen dicha información y la envían a otras áreas. Entre todas las áreas posibles que existen en un mismo sistema autónomo, debe existir de forma obligatoria, un área principal, troncal, donde confinan todas las demás áreas, denomida **backbone**. Si existiese un problema que corte el enlace entre algún router del área troncal y algún área secundaria, se debe crear un enlace virtual que posibilite la continuidad de las funciones del área troncal como área principal.

OSPF mantiene actualizada la capacidad de encaminamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- Paquetes Hello (tipo 1): cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.
- Paquetes de descripción de base de datos estado-enlace o DataBase Description o DBD (tipo 2): se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.
- Paquetes de estado-enlace o Link State Advertisements (LSA): los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA.



Border Gateway Protocol BGP

El enrutamiento basado en el vector distancia y en de estado del enlace son protocolos intradomino, por lo que no se pueden utilizar entre sistemas autónomos. Estos dos protocolos no son adecuados para encaminamiento entre dominios debido fundamentalmente a problemas de escalabilidad. Estos dos protocolos se vuelven inestables cuando el dominio de operación se hace muy grande. En encaminamiento basado en vector distancia no es posible utilizar si hay más de cierta cantidad saltos; y el encaminamiento basado en el estado del enlace necesita gran cantidad de recursos para calculas las tablas de encaminamiento, al mismo tiempo que crea un excesivo tráfico de datos debido a la inundación de información de las redes que las componen. Por esto, es necesario un tercer protocolo denominado encaminamiento basado en el vector camino.

El **encaminamiento basado en el vector camino** es un algoritmo de enrutamiento interdominio, que asume que existe un nodo que cumple el papel de nodo central del sistema autónomo, y que actúa en nombre de todo el sistema. Este nodo, denomiado **nodo speaker**, crea en un sistema autónomo una tabla de encaminamiento y la pública a todos los nodos speaker de los sistemas autónomos vecinos. El funcionamiento de este algoritmo es similar al del vector distancia, con la diferencia que solo los nodos speakers pueden comunicarse entre ellos, enviándose información de sus tablas de enrutamiento, con el fin de que los demas sistemas autónomos conozcan la distribución de cada sistema. Este método es más eficiente que los dos anteriores, ya que no requiere de una comunicación de grandes cantidades de datos continuamente, sino que se realiza de forma periódica con cada cambio en la red.

El BGP, **Protocolo de Pasarela Frontera**, es un protocolo interdominio que utiliza el encaminamiento basado en el vector camino. El intercambio de información se realiza mediante el establecimiento de una sesión de comunicación entre los routers de borde de los sistemas autónomos. Una sesión es una conexión

que se establece entre dos routers BGP solo para el intercambio de infromacion de encaminamiento. Para conseguir una entrega fiable de la información, se hace uso de una sesión de comunicación basada en TCP. Esta sesión debe mantenerse conectada debido a que ambos extremos de la comunicación periódicamente se intercambian y actualizan información.

BGP puede utilizar dos tipos de sesiones, sesiones externas (E-BPG) y sesiones internas (I-BGP). Las **sesiones externas** se utilizan para intercambiar información entre dos nodos speakers, con el objetivo de hacer posible que los sistemas autónomos conozcan las distintas redes que existen; mientras que la **sesión interna**, por otro lado, se utiliza para intercambiar información entre dos routers dentro de un mismo sistema autónomo.

Capa de Transporte

El nivel de transporte constituye el cuarto nivel del modelo OSI. Los protocolos de este nivel se encargan de la entrega de datos desde un programa de aplicación situado en un dispositivo a otro programa de aplicación situado en otro dispositivo. Actúa como un enlace entre los protocolos de los niveles superiores (sesión, presentación y de aplicación) y los servicios ofrecidos por los niveles inferiores (de red, de enlace de datos y físico). Los niveles superiores pueden utilizar los servicios del nivel de transporte para interactuar con la red sin tener que interactuar o preocuparse directamente con la existencia ele los niveles inferiores. Para que esta separación sea posible, el nivel de transporte es independiente de la red física.

La capa da transporte identifica unívocamente cada entidad de sesión por su dirección de transporte. El servicio de transporte provee de medios para establecer, mantener y liberar conexiones de transporte. Los siguientes servicios son provistos por la capa de transporte:

- establecimiento de la conexión – transporte
- transferencia de datos
- liberación de la conexión – transporte

La capa de transporte incluye estas funciones:

- mapeado de las direcciones de transporte dentro de las direcciones de red
- multiplexado end-to-end de conexiones de transporte dentro de conexiones de red
- establecimiento y liberación de conexiones de transporte
- end-to-end para segmentación, bloques y concatenación
- funciones de supervisión
- transferencia de unidades de servicios de datos
- control de flujo de mensajes
- retransmisión de paquetes

El nivel de transporte está representado en TCP/IP por dos protocolos: TCP y UDP. De estos, UDP es el más simple; ofrece una funcionalidad de transporte que no asegura secuencia, cuando la fiabilidad y la seguridad son menos importantes que el tamaño y la velocidad. La mayoría de las aplicaciones, sin embargo, requieren una entrega extremo a extremo fiable y hacen uso de TCP.

Los protocolos de transporte del conjunto ele protocolos TCP/IP definen un conjunto de conexiones conceptuales para los procesos individuales denominados puertos del protocolo o sencillamente puertos. Un puerto es un punto de destino (normalmente un buffer) que almacena datos para ser utilizados por un proceso particular. La interfaz entre los procesos y sus puertos correspondientes es ofrecida por el sistema operativo de la estación.

El protocolo IP es un protocolo estación a estación, lo que significa que puede entregar un paquete de un dispositivo físico a otro. Los protocolos de nivel de transporte de TCP/IP son protocolos puerto a puerto, que trabajan encima de los protocolos IP para entregar el paquete desde un puerto origen a los servicios IP en el comienzo de la transmisión y desde los servicios IP al puerto de destino en el final

Transmission Control Protocol TCP

El **protocolo de control de transmisión** es un protocolo de transporte orientado a la conexión que, al implementar un control de flujo y errores a nivel de transporte, se define también como fiable. TCP está diseñado para proporcionar una comunicación segura entre pares de procesos (usuarios TCP) a través de una gran variedad de redes interconectadas. Existe el interrogante de como TCP es un protocolo orientado a la conexión, si se encuentra basado en IP, un protocolo no orientado a la conexión. Esto se debe a que TCP establece conexiones virtuales, y solo usa los servicios de IP para transmitir los segmentos individuales al receptor. Es TCP quien controla la conexión entre ellos.

Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos.

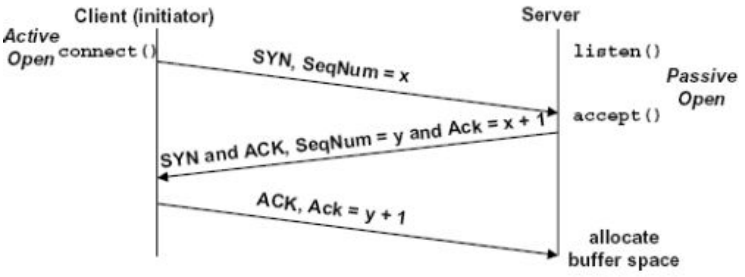
TCP suministra dos facilidades útiles para etiquetar datos: cargar y urgente:

- **Cargar flujo de datos**: normalmente, TCP decide cuándo se han acumulado suficientes datos para formar un segmento para su transmisión. El usuario TCP puede requerir que TCP transmita todos los datos pendientes a los que incluye una etiqueta con un indicador de carga. En el extremo receptor, TCP entregará los datos al usuario en la misma forma. Un usuario puede requerir esto si en los datos se detecta una interrupción lógica.
- **Indicación de datos urgentes**: esta posibilidad proporciona un medio para informar al usuario TCP destino que en el flujo de datos entrantes existen datos significativos o «urgentes». Es responsabilidad de usuario destino realizar la acción apropiada. Para especificar que un dato se debe enviar de forma urgente, se coloca el bit URG activado.

En TCP la transmisión orientada a la conexión consta de tres partes: establecimiento de la conexión, transferencia de datos y cierre de la conexión.

Establecimiento de la conexión

TCP transmite los datos en modo full dúplex, lo que permite que, cuando dos terminales se conectan, puedan enviarse segmentos entre si simultáneamente. Esto implica que cada parte debe inicializar la comunicación y obtener la aprobación desde la otra parte antes de transferir datos.



El establecimiento de la conexión en TCP se da a partir de lo denominado **Negociación en tres sentidos**.

El proceso comienza en el servidor. El programa servidor le dice a su TCP que está listo para aceptar una conexión, pero que necesita de un programa cliente que los conecte. A esto se lo denomina *apertura pasiva*.

El programa emite una petición para una *apertura activa*. Un cliente que quiere conectarse a un servidor ya abierto, le dice a su TCP que necesita conectarse a un servidor particular. Para esto, TCP lleva a cabo la negociación en tres pasos como sigue:

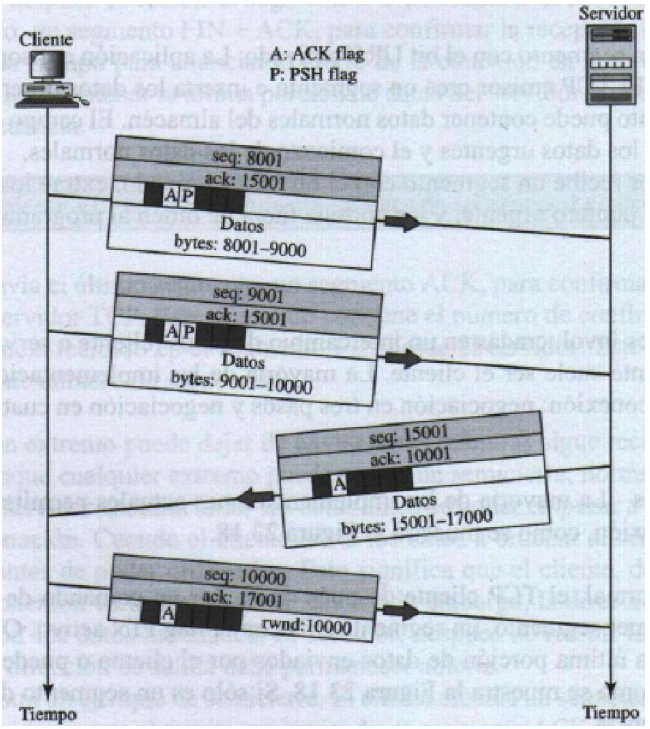
1. El cliente envía el primer segmento en donde solo el campo SYN está activo (segmento SYN). Consume un número de secuencia. Este segmento es para sincronizar los números de secuencia. Cuando comienza la trasferencia, el número de secuencia se incrementa en uno.
2. El servidor envía un segundo segmento, un segmento denominado SYN + ACK, con 2 bits activos: SYN y ACK. Este segmento cumple un doble objetivo, comunicación en la dirección contraria, y confirmación del segmento SYN anterior. Consume el número de secuencia.

3. El cliente envía el tercer segmento. Es un solo segmento ACK. Confirma la recepción del segmento con el flag ACK y el campo de confirmación. El número de secuencia de este segmento es el mismo que el primero segmento (segmento SYN). El segmento ACK no consume ningún número de secuencia.

Una conexión está únicamente determinada por los puertos origen y destino. Así, en cualquier instante de tiempo, solamente puede haber una única conexión TCP entre un único par de puertos. Sin embargo, un puerto dado puede admitir múltiples conexiones, cada una con diferentes puertos.

Transferencia de datos

Después que la conexión se haya establecido, tanto el cliente como el servidor pueden efectuar la transmisión de datos bidireccional, es decir, cualquiera de las partes pueden enviar datos y confirmaciones: los datos que viajan en la misma dirección que una confirmación se envían en el mismo segmento. En el ejemplo que representa la imagen, el cliente envía 2000 bytes utilizando dos segmentos distintos. El servidor envía 2000 bytes en un mismo segmento. El cliente envía un segmento más. Los tres primeros segmentos transportan datos y confirmaciones, pero el último segmento solo lleva una confirmación, ya que no hay más datos que enviar.



Los números de segmento de los dos primeros segmentos enviados deben ser correlativos, con el fin de representar que son parte de un mismo paquete. El último segmento enviado por el cliente es una confirmación. Esto implica que, al no enviar datos, el número de secuencia será el mismo que el número de secuencia del último dato enviado. El valor del ACK será el número de secuencia siguiente al último dato recibido del servidor, con el fin de indicar que dicho segmento se recibió en correctas condiciones.

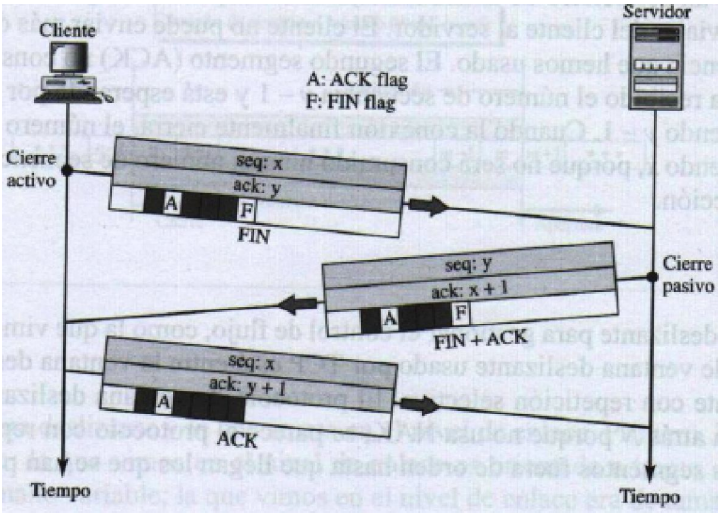
El TCP emisor utiliza un buffer de almacenamiento para guardar el flujo de datos que vienen desde el programa de aplicación. Es el TCP emisor quien define el tamaño del segmento. El TCP receptor tambien almacena los datos a medida que van llegando en un buffer, y se los entrega al programa de aplicación cuando esté listo, o cuando es conveniente para el TCP receptor. El bit PSH (pushing) permite gestionar esta flexibilidad haciendo que el TCP emisor no deba esperar a rellenar su ventana para transmitir: debe crear un segemento y enviarlo inmediatamente. En este segmento, se coloca activo el bit PSH, el cual indica en el receptor que el segmento incluye datos que deben ser entregados lo antes posible al programa de aplicación receptor.

TCP utiliza el metodo de ventana deslizante para gestionar el control de flujo, pero no es identica a la utilizada en la capa de enlace. Es una mezcla entre go back to N, porque no utiliza NAK, y repeticion selectiva porque el receptor mantiene los segmentos fuera de orden hasta que llegan todos los que se han pedido. A su vez, esta implementacion de ventana deslizante es orientada al byte y permite un tamaño de ventana variable; mientras que la ventana deslizante de la capa de enlace es orientada a la trama, y es de tamaño fijo.

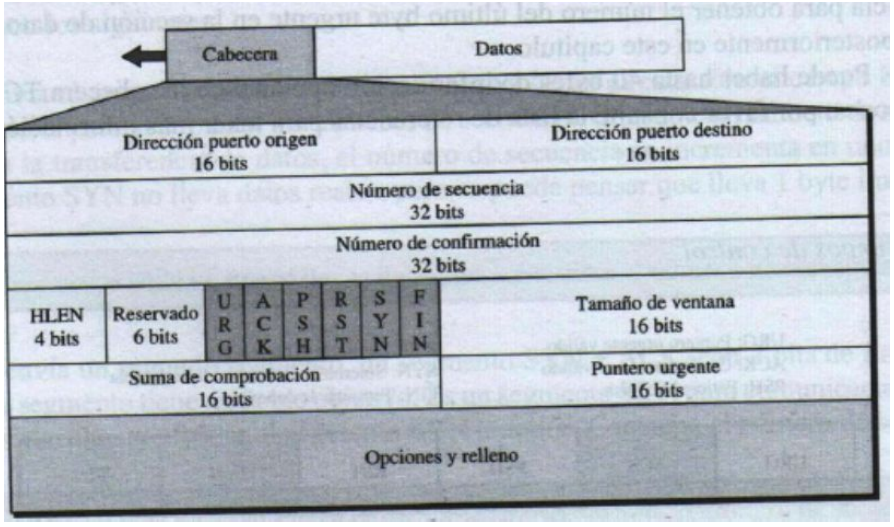
Como TCP debe proporcionar fiabilidad en la transferencia, utiliza un método de control de errores, consistente en la implementación de checksums, confirmación de recepción de segmentos, y retransmisión de segmentos cuando uno se ha corrompido, perdido o retrasado.

Fin de la conexión

Cualquiera de las dos partes involucradas en una conexión puede darle cierre. Al igual que el establecimiento de la conexión, el fin de la conexión se da utilizando la negociación en tres pasos:



1. En una situación normal, el TCP cliente, después de recibir una solicitud de cierre del proceso cliente, envía un segmento FIN con el flag FIN activo. Este segmento puede incluir la última porción de datos. Si solo se trata de un segmento de control que indica el fin de la conexión, consume un solo número de secuencia.
2. El servidor TCP, después de recibir el segmento FIN, informa a su proceso de la situación y envía el segundo segmento, un segmento FIN + ACK para confirmar la recepción del primer segmento desde el cliente, y al mismo tiempo, anunciar el cierre de la conexión en la dirección contraria. Este segmento también puede contener la última porción de datos. Si no lleva datos, consume un único número de secuencia.
3. El cliente TCP envía el último segmento, un segmento ACK, para confirmar la recepción del segmento FIN del servidor TCP. Este segmento contiene el número de confirmación, que es uno más que el número de secuencia recibido en el segmento FIN desde el servidor. Este segmento no puede llevar datos, y no consume números de secuencia.



User Datagram Protocol UDP

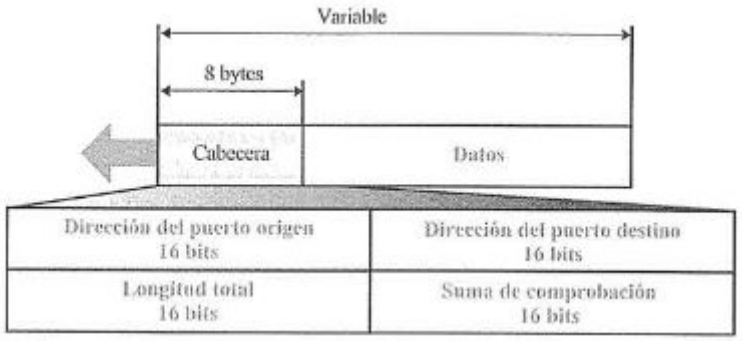
El **Protocolo de Datagrama de Usuario** es un protocolo sin conexión y no fiable. No añade a los servicios de IP, excepto proporcionar comunicación proceso a proceso en lugar de comunicaciones computadora a computadora, y de añadir información sobre direcciones de puertos, control de errores mediante sumas de comprobación y la información de longitud de los datos del nivel superior. UDP es un protocolo sencillo que añade un mínimo de sobrecarga. Si se busca enviar un dato pequeño, en el que la confiabilidad no cumple un papel fundamental, es mejor utilizar UDP por sobre TCP, ya que implica mucho menos interacción entre emisor y receptor.

UDP proporciona sólo las funciones básicas necesarias para la entrega extremo a extremo de una transmisión. No ofrece funciones de secuenciamiento ni de reordenación y no puede especificar el paquete dañado cuando se informa de un error (por lo que debe usarse con lCMP). UDP puede descubrir que ha ocurrido un error; ICMP puede, a continuación, informar al emisor de que un datagrama ele usuario se ha dañado o se ha descartado. Tampoco tiene, sin embargo, la capacidad para especificar qué paquete se ha

perdido. UDP contiene solo una suma de comprobación; no contiene un identificador o número de secuencia para un segmento de datos concreto.

UDP es un protocolo no orientado a conexión. Es decir, cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber realizado previamente una conexión con la máquina de destino (maquina B), y el destinatario recibirá los datos sin enviar una confirmación al emisor (la maquina A). Esto es debido a que la encapsulación de datos enviada por el protocolo UDP no permite transmitir la información relacionada al emisor. Por ello el destinatario no conocerá al emisor de los datos excepto su IP.

Este protocolo es utilizado cuando un proceso necesita una comunicación petición- respuesta sencilla, y no le preocupa el control de flujo y errores. Habitualmente, no se usa en envío de datos masivos. UDP es un protocolo de transporte adecuado para multienvio. Se usa para procesos de gestión como SNMP y protocolos de actualización de ruta como RIP.



~~DHCP~~

~~Conexiones remotas : protocolos-> rlogin, telnet, ssh~~

~~NMS – SNMP~~

QoS

Seguridad

DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Puertos	67/UDP (servidor) 68/UDP (cliente)
Ubicación en la pila de protocolos	
Aplicación	**DHCP**
Transporte	UDP
Red	IP

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

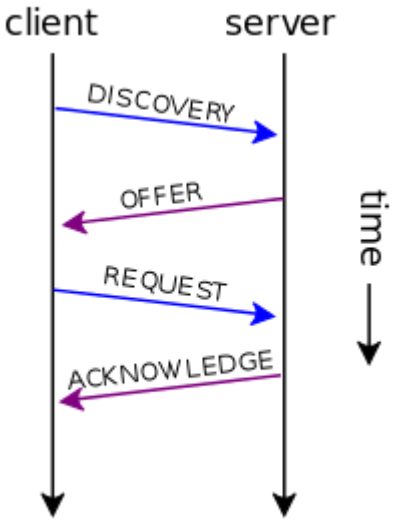
Asignación manual o estática: El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

Asignación automática: Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

Asignación dinámica: El único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

Cómo funciona el protocolo DHCP

Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP fija. Por lo tanto, en una red puede tener solo un equipo con una dirección IP fija: el servidor DHCP.



El sistema básico de comunicación es BOOTP (protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente). Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en broadcast con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local. Cuando el DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión que contiene toda la información solicitada por el cliente.

Se podría suponer que un único paquete es suficiente para que el protocolo funcione. En realidad, hay varios tipos de paquetes DHCP que pueden emitirse tanto desde el cliente hacia el servidor o servidores, como desde los servidores hacia un cliente:

- DHCPDISCOVER (para ubicar servidores DHCP disponibles)

- DHCPOFFER (respuesta del servidor a un paquete DHCPDISCOVER, que contiene los parámetros iniciales)
- DHCPREQUEST (solicitudes varias del cliente, por ejemplo, para extender su concesión)
- DHCPACK (respuesta del servidor que contiene los parámetros y la dirección IP del cliente)
- DHCPNAK (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea)
- DHCPDECLINE (el cliente le anuncia al servidor que la dirección ya está en uso)
- DHCPRELEASE (el cliente libera su dirección IP)
- DHCPINFORM (el cliente solicita parámetros locales, ya tiene su dirección IP)

El primer paquete emitido por el cliente es un paquete del tipo DHCPDISCOVER. El servidor responde con un paquete DHCPOFFER, fundamentalmente para enviarle una dirección IP al cliente. El cliente establece su configuración y luego realiza un DHCPREQUEST para validar su dirección IP (una solicitud de transmisión ya que DHCPOFFER no contiene la dirección IP). El servidor simplemente responde con un DHCPACK con la dirección IP para confirmar la asignación. Normalmente, esto es suficiente para que el cliente obtenga una configuración de red efectiva, pero puede tardar más o menos en función de que el cliente acepte o no la dirección IP.

Conexiones Remotas

Rlogin

El protocolo Rlogin es un protocolo similar a Telnet, con la diferencia fundamental que Rlogin utiliza servicios UDP y Telnet usa servicios TCP en la capa de transporte. El protocolo Rlogin permite a los usuarios iniciar la sesión en un sistema principal remoto y utilizar los terminales como si estuvieran conectados directamente al sistema principal remoto.

Telnet

El protocolo **Telnet** (Telecommunications Network) es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente con un intérprete de comandos del lado del servidor.

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

Telnet es un protocolo base al que se le aplican otros protocolos del conjunto TCP/IP. Las especificaciones Telnet no mencionan la autenticación ya que se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet). Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada). Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

Excepto por las opciones asociadas y las reglas de negociación, las especificaciones del protocolo Telnet son básicas. La transmisión de datos a través de Telnet consiste sólo en transmitir bytes en el flujo TCP. El protocolo Telnet especifica que los datos deben agruparse de manera predeterminada en un búfer antes de enviarse.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH, que puede describirse como una versión cifrada de telnet.

Funcionamiento

- Se puede utilizar en varias plataformas UNIX, Windows y Linux
- El comando para iniciar una sesión Telnet:

> telnet nombre_del_servidor
> telnet 125.64.124.77
> telnet 125.64.124.77 80

SSH

SSH (Secure SHell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas. Puede ser utilizado también para la transferencia de archivos usando SFTP o SCP. Se le asigna el puerto 22, y funciona sobre el estándar TCP.

Al establecerse la conexión SSH queda formado un túnel entre ambos equipos, es decir, sólo entra al mismo quien tenga permiso, y todo aquel que pueda capturar su tráfico no debe tener forma de interpretarlo, ni modificarlo, ni desviarlo de su destino. Al crear un túnel, se establece una red particular entre ambos (VPN, Virtual Private Network).

Existen 2 versiones de SSH, la versión 1 de SSH hace uso de muchos algoritmos de cifrado patentados (sin embargo, algunas de estas patentes han expirado) y es vulnerable a un agujero de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicación. La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de claves mejorado que no es vulnerable al agujero de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.

Funcionamiento

- El cliente inicia una conexión TCP sobre el puerto 22 del servicio
- El cliente y servidor se ponen de acuerdo en la versión de protocolo a utilizar y el algoritmo de cifrado.
- El servidor manda su clave pública al cliente.

Network Management System

Las actuales redes de telecomunicación se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que los componen. Los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento y la planificación estratégica de su crecimiento. Debido a dicho crecimiento, la gestión de red integrada se ha convertido en un aspecto de enorme importancia en el mundo de las telecomunicaciones, y para esto es que se desarrolló un sistema de administración de redes, NMS.

ISO define cinco áreas funcionales a las que el NMS enfoca sus funciones:

- **Administración de fallos**: detecta, aísla, notifica y corrige fallas encontradas en la red.
- **Gestión de la configuración**: se encarga de aspectos relacionados con la configuración de los dispositivos de red, como la gestión de archivos de configuración, gestión de inventario y gestión de software.
- **Gestión del Desempeño**: Monitorear y medir diversos aspectos de la perfomance de la red, para que el desempeño general pueda mantenerse en un nivel aceptable.
- **Administración de seguridad**: proporciona el acceso a dispositivos de red y a recursos corporativos solo a personas autorizadas.
- **Contabilidad**: mantiene información acerca del uso de los recursos de la red.

Los sistemas de gestión de redes se basan en los términos gestor, agente, base de información de gestión y protocolo de gestión de red.

La estación de gestión, **gestor**, es normalmente un dispositivo autónomo pero puede ser implementado en un sistema compartido. En cualquier caso, la estación de gestión sirve como interfaz entre el gestor de red humano y el sistema de gestión de red. El gestor tiene acceso a los valores de esta base de datos. Por

ejemplo, un encaminador puede almacenar en variables adecuadas el número de paquetes recibidos y reenviados. El gestor puede leer y comparar los valores de estas dos variables para ver si el encaminador se encuentra congestionado o no. El gestor puede también hacer que el encaminador realice ciertas acciones. Por ejemplo, un encaminador periódicamente comprueba el valor del contador de reinicios para ver cuándo debería reiniciarse. Se reinicia, por ejemplo, si el valor del contador es 0. El gestor puede utilizar esta característica para reiniciar el agente de forma remota en cualquier instante. Simplemente envía un paquete para forzar un valor igual a 0 en el contador.

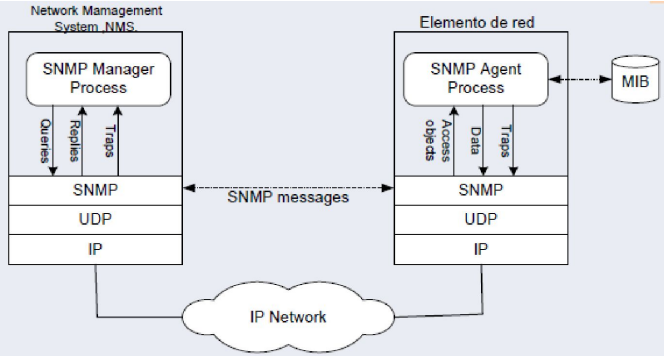
El otro elemento activo en un sistema de gestión de red es el **agente**. Las plataformas claves, como los computadores, puentes, dispositivos de encaminamiento y concentradores se pueden equipar con software de agente para que puedan ser gestionados desde la estación de gestión. El agente responde a las solicitudes de información desde una estación de gestión, responde a las solicitudes de acción desde la estación de gestión y puede, de una forma asíncrona, proporcionar a la estación de gestión información importante y no solicitada.

El medio por el cual se pueden gestionar los recursos de una red es representando estos recursos como objetos. Cada objeto es, esencialmente, una variable de datos que representa un aspecto del agente de gestión. La colección de objetos se conoce como **base de información de gestión** (MIB, Management Information Base). La MIB funciona como una colección de puntos de accesos al agente por parte de la estación de gestión. Estos objetos están normalizados a través de los sistemas de una clase particular (sistema, interfaz, traducción de direcciones, IP, ICMP, TCP, UDP Y EGP). La estación de gestión lleva a cabo la función de monitorización mediante el acceso a los valores de los objetos MIB. Una estación de gestión puede causar que una acción tenga efecto en un agente o puede cambiar la configuración de un agente mediante la modificación de los valores de variables específicas.

La estación de gestión y el agente están enlazados por el protocolo de gestión de red. El protocolo utilizado para la gestión en redes TCP/IP es el protocolo sencillo de gestión de red (SNMP).

Protocolo sencillo de gestión de red

El **Protocolo Sencillo de Gestión de Red** (SNMP, Simple Network Management Protocol) es un marco de trabajo para gestionar los dispositivos en una internet que utiliza el conjunto de protocolos TCP/IP. Ofrece un conjunto de operaciones fundamentales para monitorizar y mantener una red internet.



SNMP es un protocolo del nivel de aplicación en el que unas pocas estaciones gestoras controlan un conjunto de agentes. El protocolo se encuentra diseñado en el nivel de aplicación para que pueda monitorizar dispositivos de diferentes fabricantes e instalados en redes físicas distintas. En otras palabras, SNMP libera a las tareas de gestión de las características físicas de los dispositivos gestionados y de la tecnología de red subyacente. Se puede emplear en una red internet heterogénea compuesta por diferentes LAN y WAN conectadas por encaminadores o pasarelas de diferentes fabricantes.

SNMP se basa en tres primitivas que permite la comunicación entre el agente y el gestor. Estas primitivas son

- **Get**: permite a la estación de gestión obtener del agente los valores de objetos.
- **Set**: permite a la estación de gestión establecer valores de objetos del agente.
- **Notify**: permite a un agente notificar a una estación de gestión la producción de eventos significativos.

Como el nombre sugiere, SNMP es una herramienta sencilla para la gestión de red. Define una base de información de gestión (MIB) limitada y fácil de implementar de variables escalares y tablas de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB y para

permitir a un agente emitir notificaciones no solicitadas, llamadas intercepciones (traps). Esta simplicidad es la potencia de SNMP. SNMP se implementa de una forma fácil y consume un tiempo modesto del procesador y de recursos de red. También, la estructura del protocolo y de la MIB es suficientemente directa de forma que no es difícil alcanzar la interacción entre estaciones de gestión y software de agente de varios vendedores.

Con una utilización tan amplia, las deficiencias de SNMP han llegado a ser bastante aparentes; éstas incluyen deficiencias funcionales y la falta de una herramienta de seguridad. Como resultado en 1993 se publicó una versión mejorada, conocida como SNMPv2, y en 1996 se publicó una versión revisada

SNMPv2

Sorprendentemente, SNMPv2 no proporciona gestión de red. En lugar de eso SNMPv2 proporciona un marco de trabajo en el que se pueden construir aplicaciones de gestión de red. Estas aplicaciones, como la gestión de fallos, monitorización del rendimiento, contabilización de tiempo, etc. están fuera del ámbito del estándar. Lo que proporciona SNMPv2 es la infraestructura de la gestión de red, a la vez de definir la estructura del MIB y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI, Structure of Management Information). Podemos pensar que esto constituye el lenguaje para definir la información de gestión.

El corazón del entorno de trabajo de SNMPv2 es el protocolo mismo. El protocolo proporciona un mecanismo básico y directo para intercambiar información de gestión entre un gestor y un agente. La unidad básica de intercambio es el mensaje, que consta de un envoltorio de mensaje exterior y una unidad de datos de protocolo interior (PDU). La cabecera de mensaje exterior está relacionada con la seguridad y se discute posteriormente en esta sección.

Todos estos intercambios se realizan utilizando el protocolo SNMPv2, que es un protocolo sencillo del tipo petición/respuesta. Normalmente, se implementa encima del protocolo de datagrama de usuario (UDP), que es parte del conjunto de protocolos TCP/IP. Ya que los intercambios SNMPv2 son del tipo de pares solicitudrespuesta discretos, no se requiere una conexión segura.

SNMPv3

Muchas de las deficiencias funcionales de SNMP se solucionaron en SNMPv2. Para corregir las deficiencias en seguridad de SNMPvl/SNMPv2, se publicó SNMPv3 como un conjunto de Estándares Propuestos en enero de 1998 (actualmente RFC 2570 a 2575). Este conjunto de documentos no proporciona una capacidad SNMP completa si no que define una arquitectura general de SNMP y un conjunto de capacidades en seguridad. Éstas están pensadas para que se utilicen con el SNMPv2 actual.

SNMPv3 proporciona tres servicios importantes: autentificación, privacidad y control de acceso. Los dos primeros forman parte del modelo de Seguridad Basada en Usuarios (USM, UserBased Sccurity) y el último se define en el Modelo de Control de Acceso Basado en Consideraciones (VACM, ViewBased Access Control Model).

El **mecanismo de autentificación** en USM asegura que el mensaje recibido lo transmitió el director cuya identidad aparece como fuente en la cabecera del mensaje. Este mecanismo también asegura que el mensaje no se ha alterado en la transmisión y que no se ha retardado o retransmitido artificialmente. El director que envía proporciona la autentificación mediante la inclusión de un código de autentificación del mensaje con el mensaje SNMP que envía.

El **servicio de privacidad** de USM habilita a los gestores y a los agentes a encriptar mensajes. De nuevo, el gestor director y el agente director deben compartir una clave secreta. En este caso, si los dos están configurados para utilizar la facilidad de privacidad, todo el tráfico entre ellos es encriptado utilizando el estándar de encriptado de datos (DES).

El servicio de control de acceso hace posible configurar los agentes para que proporcionen diferentes niveles de acceso a la base de información de gestión (MIB) del agente a diferentes gestores. Un director agente puede restringir el acceso a su MIB a un director gestor de dos formas. Primero, puede restringir el

acceso a cierta porción de su MIB. Por ejemplo, un agente podría restringir a la mayoría de los gestores ver las estadísticas relacionadas con el rendimiento y permitir solamente a un único director gestor designado para ello a ver y actualizar los parámetros de configuración. Segundo, el agente puede limitar las operaciones que un gestor podría utilizar en esa porción de la MIB. Por ejemplo, un director gestor particular podría limitar el acceso de sólolectura a una porción de la MIB de un agente.

Common Management Information Protocol

CMIP, Protocolo de Información de Administración Común (Common Management Information Protocol) desarrollado por la ISO, es otro protocolo utilizado para la administración de redes, que ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta para las 7 capas del modelo OSI.

CMIP, es considerada como una arquitectura de administración de red, que provee de mecanismos de intercambio de información, entre un administrador y elementos remotos de red, cuyo funcionamiento está basado en los servicios CMIS. Desarrollado por el Comité Consultivo Internacional de Telegrafía y Telefonía, es un protocolo similar a SNMP, sólo que con beneficios adicionales, los cuales a su vez lo hacen un protocolo complejo, que no es muy utilizado.

Dentro de las ventajas que tiene en relación con SNMP, es su manejo de seguridad integrado desde su diseño, junto con la capacidad de activar tareas cuando suceden problemas en el dispositivo administrado. Este protocolo no se basa únicamente en preguntas y respuestas, sino también en la activación de tareas.

Características del protocolo CMIP

Entre las principales características del protocolo CMIP encontramos:

- Se basa en el paradigma administrador-agente y una base de información.
- CMIS/CMIP requiere de gran cantidad de memoria y capacidad de CPU.
- Genera cabeceras complicadas en los mensajes de los protocolos.
- Las especificaciones son difíciles de realizar y tediosas de implementar en aplicaciones.
- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- Permite una jerarquía de sistemas de operación.
- El protocolo asegura que los mensajes lleguen a su destino.

Con lo anterior se tiene una administración dirigida por eventos, lo cual significa que el agente notifica al administrador de sucesos, la información concerniente a los recursos administrados. El agente es responsable de monitorear los recursos. CMIP, presenta la ventaja de que existe menor gestión de tráfico con su consecuente desventaja de tener agentes más complejos.

QoS

Acuerdo de Nivel de Servicio

Un **Acuerdo de Nivel de Servicio** (SLA, Service Level Agreement) es, simplemente, un acuerdo contractual entre una empresa de servicios y su cliente, donde se define, fundamentalmente, el servicio y los compromisos de calidad. La razón de su utilización es que los servicios de estas empresas son enormemente flexibles y versátiles, con lo que la selección de las prestaciones adecuadas es difícil y el control de calidad complejo. La consecuencia de todo esto es que las expectativas y concepto de calidad entre prestador y cliente van a diferir si no se fijan y documentan.

Ejemplo. Una empresa que tiene conectadas numerosas oficinas comerciales con su centro de proceso de datos contrata servicios de telefonía (voz) y de transmisión de datos. Para esta empresa, una interrupción del servicio de datos de 15 minutos a las 3 de la madrugada entre una oficina de segundo orden y su centro de proceso de datos puede ser irrelevante, e incluso no ser detectado por los empleados, pues a esas horas sólo se atienden unas pocas llamadas telefónicas. Pero si esa interrupción ocurre a las 12 del medio día entre la oficina comercial más importante de la empresa y el centro de proceso de datos, la cuestión puede ser bastante grave.

En ambos casos se trata de un corte de 15 minutos, pero la trascendencia ha sido muy diferente. El prestador, que se esfuerza por dar un buen servicio, considera que éste ha tenido una disponibilidad muy alta durante la semana, y está satisfecho. Pero el responsable de la oficina afectada por la interrupción a las 12 del medio día no opina lo mismo.

Sólo si hemos establecido un acuerdo de nivel de servicio donde hayamos especificado nuestras necesidades con claridad y precisión, y hayamos asumido el coste que nuestras exigencias tienen podremos discutir con fundamento si el servicio prestado está al nivel solicitado o no, y si esto es así en sólo uno de los servicios que tenemos contratados o en varios.

El SLA busca definir las propiedades con las que el servicio debe ser entregado al cliente, determinado los criterios que permitan definir si el servicio es entregado correctamente, o está sufriendo de algún defecto; las responsabilidades contractuales de ambas partes, como así también definir los límites y especificaciones técnicas para que la utilización del servicio se lleve a cabo de la mejor forma posible, bajo las necesidades del cliente.

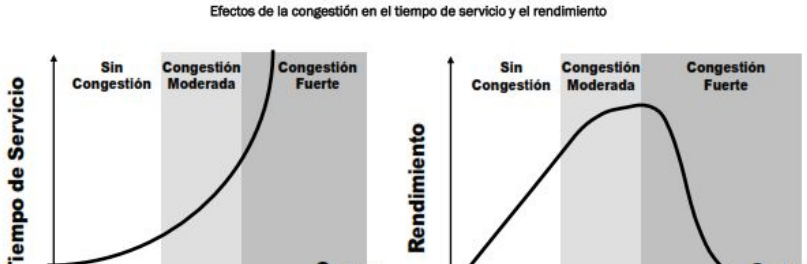
Para esto, el SLA cuenta con una serie de parámetros que permiten especificar las características del servicio otorgado:

- Timeliness
    - Delay
    - Tiempo de respuesta
    - Jitter: variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino.
- Ancho de banda
    - Tasa de datos a nivel del sistema
    - Tasa de datos a nivel de aplicación
    - Tasa de transacción: número de operaciones (solicitadas o procesadas) por segundo
- Confiabilidad
    - Tiempo medio hasta el fallo (MTTF)
    - Tiempo medio de reparación (MTTR)
    - Tiempo medio entre fallos (MTBF)
    - Porcentaje de tiempo disponible = MTTF/(MTTF + MTTR)
    - Tasa de pérdida de paquetes
    - VER

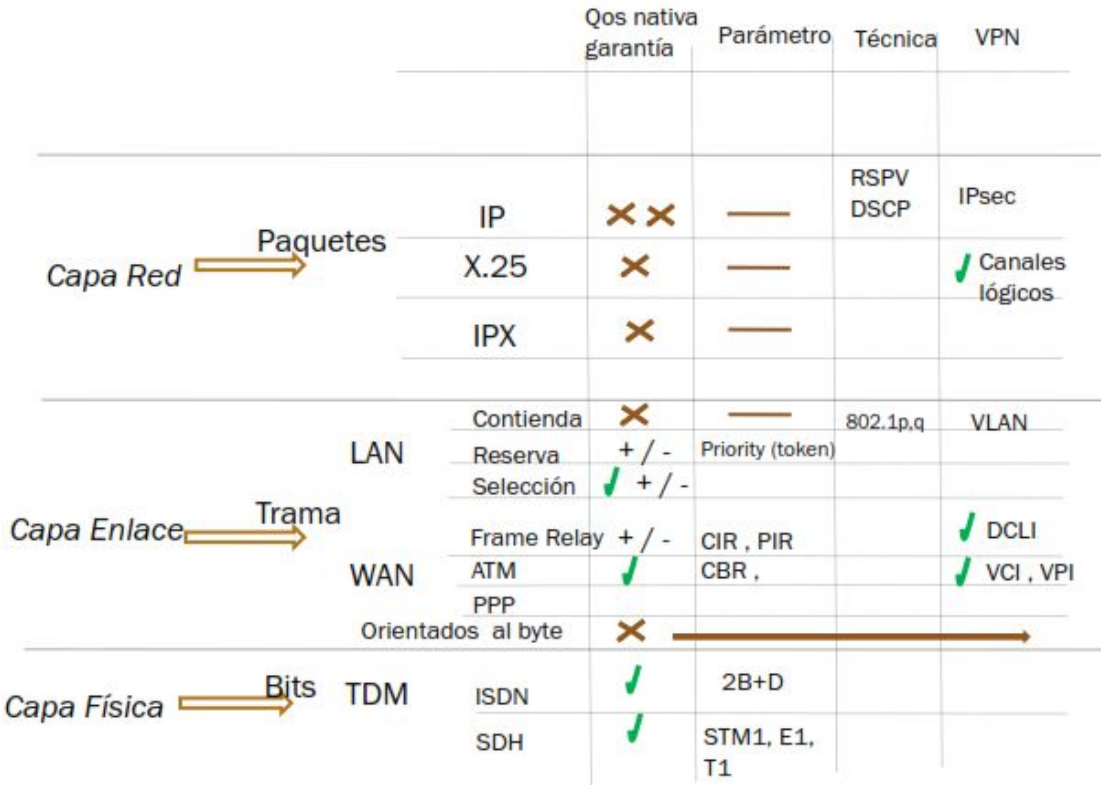
QoS en IP

QoS son las siglas de Quality of Service, un conjunto de tecnologías que garantizan la calidad de la transmisión de cierta cantidad de información en un tiempo determinado a uno o varios dispositivos. Así, QoS se encarga de priorizar el ancho de banda disponible en función de las necesidades del usuario y basándose en una serie de criterios que clasifican el tráfico. De forma puntual al protocolo de internet, QoS hace referencia a la forma en que se gestiona el ancho de banda disponible con el fin de proporcionar datos coherentes y predecibles (paquetes) a través de una red basada en IP en términos de:

- Latencia: delay, retraso maximo que una aplicación puede experimentar en la transferencia de datos.
- Jitter: variación en la latencia.
- Porcentaje de información perdida.
- Rendimiento: cantidad de información transmitida.
- Disponibilidad: tiempo en que la red se encuentra en funcionamiento.



QoS según capas del modelo OSI



Seguridad

Las necesidades de seguridad de la información en una organización han sufrido dos cambios fundamentales en las últimas décadas. Antes de la expansión del uso de equipamiento de procesamiento de datos, la seguridad de la información que una organización consideraba valiosa se proporcionaba, por un lado, por medios físicos, como el uso de armarios con cierre de seguridad para almacenar documentos confidenciales y, por otro, por medios administrativos, como los procedimientos de protección de datos del personal que se usan durante el proceso de contratación.

Con la introducción del computador, se hizo evidente la necesidad de disponer de herramientas automatizadas para la protección de archivos y otros tipos de información almacenada en el computador. Esto ocurre especialmente en el caso de sistemas compartidos como, por ejemplo, un sistema de tiempo compartido; y la necesidad se acentúa en sistemas a los que se puede acceder por medio de una red telefónica pública, una red de datos o Internet. El nombre genérico que se da al grupo de herramientas diseñadas para proteger los datos y evitar la intrusión de los hackers es el de seguridad informática.

El segundo cambio que afectó a la seguridad fue la introducción de sistemas distribuidos y el uso de redes y herramientas de comunicación para transportar datos entre el usuario de un terminal y el computador, y entre dos computadores. Las medidas de seguridad de la red son necesarias para proteger los datos durante la transmisión. De hecho, el término seguridad de la red es engañoso, en cierto modo, ya que prácticamente todas las empresas, las instituciones gubernamentales y académicas conectan sus equipos de procesamiento de datos formando un grupo de redes conectadas entre sí. Este grupo se considera con frecuencia como una red internet y se emplea el término seguridad de internet. **Seguridad de internet** consiste en las medidas para impedir, prevenir, detectar y corregir las violaciones de la seguridad que se producen durante la transmisión de la información.

La arquitectura de seguridad del modelo OSI se centra en los ataques a la seguridad, los mecanismos y los servicios, que se definen brevemente a continuación:

- Ataque a la seguridad: cualquier acción que comprometa la seguridad de la información de una organización.

- Mecanismo de seguridad: un mecanismo diseñado para detectar un ataque a la seguridad, prevenirlo o restablecerse de él.
- Servicio de seguridad: un servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización. Los servicios están diseñados para contrarrestar los ataques a la seguridad, y hacen uso de uno o más mecanismos para proporcionar el servicio.

Entonces, se define amenaza y ataque a partir de estos conceptos, como:

- Una **amenaza** es una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera generar un perjuicio. Es decir, una amenza es un posible peligro que podría explotar una vulnerabilidad.
- Un **ataque** a la seguridad de un sistema es un acto inteligente y deliberado para eludir los servicios de seguridad y violar la política de seguridad del sistema.

Ataques a la Seguridad

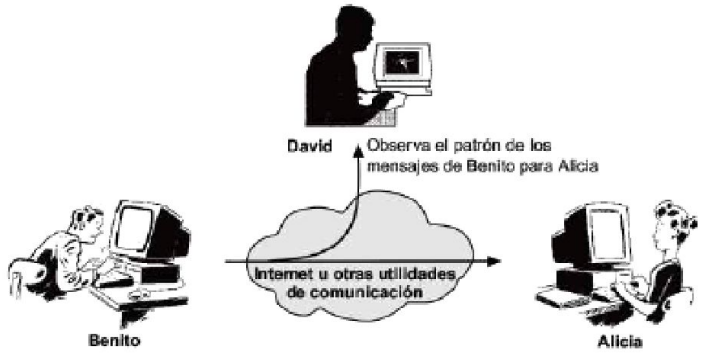
Una forma útil de clasificar los ataques a la seguridad, empleada en la recomendación X.800 y RFC 2828, es la distinción entre ataques pasivos y ataques activos. Un **ataque pasivo** intenta conocer o hacer uso de información del sistema, pero no afecta a los recursos del mismo. Un **ataque activo**, por el contrario, intenta alterar los recursos del sistema o afectar a su funcionamiento

Ataques Pasivos

Los ataques pasivos se dan en forma de escucha o de observación no autorizadas de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo. Dos tipos de ataques pasivos son la obtención de contenidos de mensajes y el análisis del tráfico.

La obtención de contenidos de mensajes se entiende fácilmente como que un oponente intenta conocer los contenidos de transmisiones vía conversación telefónica, un mensaje por correo electrónico o cualquier fichero enviado.

(a) Obtención del contenido del mensaje



(b) Análisis del tráfico

Un segundo tipo de ataque pasivo, el análisis de tráfico, es más sutil. Supongamos que hemos enmascarado los contenidos de los mensajes u otro tráfico de información de forma que el oponente, incluso habiendo capturado el mensaje, no pueda extraer la información que contiene. La técnica común para enmascarar los contenidos es el **cifrado**. Incluso si tuviésemos protección mediante cifrado, un oponente podría observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y la longitud de los mensajes que se están intercambiando. Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar.

Los ataques pasivos son muy difíciles de detectar ya que no implican alteraciones en los datos. Normalmente, el mensaje se envía y se recibe de una forma aparentemente normal y ni el emisor ni el receptor son conscientes de que una tercera persona ha leído los mensajes o ha observado el patrón del tráfico. Sin embargo, es posible evitar el éxito de estos ataques, normalmente mediante el uso del cifrado. Así, al tratar con los ataques pasivos, el énfasis se pone más en la prevención que en la detección.

Ataques Activos

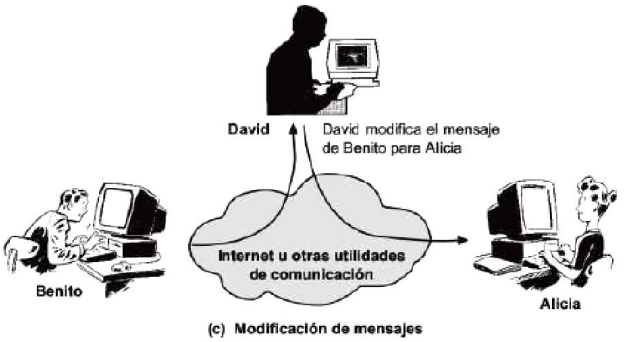
Los ataques activos implican alguna modificación del flujo de datos o la creación de un flujo falso y se pueden dividir en cuatro categorías: suplantación de identidad, repetición, modificación de mensajes e interrupción de servicio.

Una **suplantación** se produce cuando una entidad finge ser otra. Un ataque de este tipo incluye habitualmente una de las otras formas de ataque activo. Por ejemplo, las secuencias de autentificación pueden ser capturadas y repetidas después de que una secuencia válida de autentificación haya tenido lugar, permitiendo así, que una entidad autorizada con pocos privilegios obtenga privilegios extra haciéndose pasar por la entidad que realmente los posee.

La **repetición** implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado.

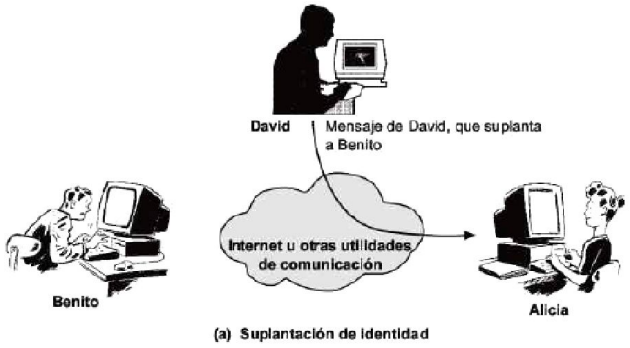
La **modificación de mensajes** significa que una parte de un mensaje original es alterada, o que los mensajes se han retrasado o reordenado, para producir un efecto no autorizado (Figura 1.2c). Por ejemplo, el mensaje «Permitir a Carlos Pérez que lea las cuentas de archivos confidenciales» se modifica para convertirlo en «Permitir a Marcos Fernández que lea las cuentas de archivos confidenciales».

La **interrupción del servicio** impide el uso o la gestión normal de las utilidades de comunicación (Figura 1.2d). Este ataque podría tener un objetivo específico; por ejemplo, una entidad podría suprimir todos los mensajes dirigidos a un destino en particular (por ejemplo, el servicio de auditoría de la seguridad). Otra forma de este tipo de ataque es la interrupción de una red completa, ya sea inhabilitándola o sobrecargándola con mensajes para reducir su rendimiento.

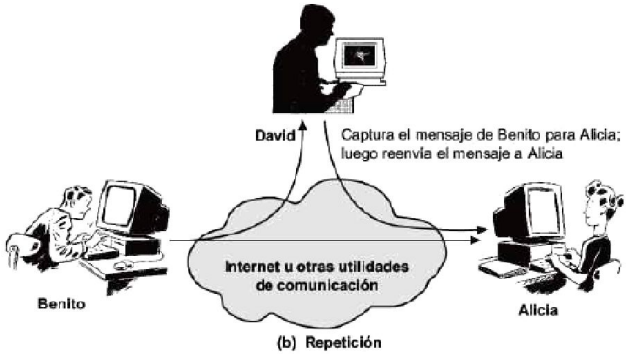


(c) Modificación de mensajes

(d) Interrupción de servicio



(a) Suplantación de identidad



(b) Repetición

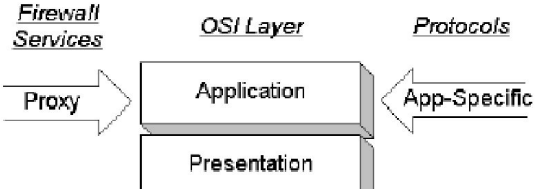
Firewalls

Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

OSI Layer	*Policy Criteria*	*Firewall Service*
Presentation	<none>	<none>
Session	- User Identity	- User mapping (gateway) - User filtering



Sniffers

Un problema de seguridad significativo para los sistemas en red es el acceso hostil, o al menos no autorizado, por parte de usuarios o software, los que buscan "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet. A esto se lo llama **sniffing**.

Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interactuación con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, etc.).

Por ello, cada vez es más importante enviar encriptada la información. Por ejemplo, los mensajes de correo electrónico y archivos delicados deben enviarse encriptados con PGP o GnuPG. La transferencia de archivos mediante FTP, debe evitarse en lo posible, utilizando SSH.

Esto limita el alcance del sniffer, pues en este caso no podrá captar el tráfico externo a la red (osea, más allá de los routers y dispositivos similares), y dependiendo de donde esté conectado en la Intranet, podrá acceder a más datos y más importantes que en otro lugar. Para absorber datos que circulan por Internet, lo que se hace es crear servidores de correo o de DNS para colocar sus sniffers en estos puntos tan estratégicos. La cantidad de tramas que puede obtener un sniffer depende de la topología de red, del modo donde esté instalado y del medio de transmisión. Por ejemplo:

- Para redes antiguas con topologías en estrella, el sniffer se podría instalar en cualquier nodo, ya que lo que hace el nodo central es retransmitir todo lo que recibe a todos los nodos. Sin embargo en las redes modernas, en las que solo lo retransmite al nodo destino, el único lugar donde se podría poner el sniffer para que capturara todas las tramas sería el nodo central.
- Para topologías en anillo, doble anillo y en bus, el sniffer se podría instalar en cualquier nodo, ya que todos tienen acceso al medio de transmisión compartido.
- Para las topologías en árbol, el nodo con acceso a más tramas sería el nodo raíz, aunque con los switches más modernos, las tramas entre niveles inferiores de un nodo viajarían directamente y no se propagarían al nodo raíz.

Algunos sniffers trabajan sólo con paquetes de TCP/IP, pero hay otros más sofisticados que son capaces de trabajar con un número más amplio de protocolos e incluso en niveles más bajos tal como el de las tramas del Ethernet. El modo más sencillo de comprender su funcionamiento, es examinando la forma en que funciona un sniffer en una red Ethernet. Se aplican los mismos principios para otras arquitecturas de red.

Un sniffer de Ethernet es un programa que trabaja en conjunto con la tarjeta de interfaz de red (NIC, Network Interface Card), para absorber indiscriminadamente todo el tráfico que esté dentro del umbral de audición del sistema de escucha. Y no sólo el tráfico que vaya dirigido a una tarjeta de red, sino a la dirección de difusión de la red 255.255.255.255 (broadcast).

Para ello, el sniffer tiene que conseguir que la tarjeta entre en modo "promiscuo", en el que recibirá todos los paquetes que se desplazan por la red. Así pues, lo primero que hay que hacer es colocar el hardware de la red en modo promiscuo; a continuación el software puede capturar y analizar cualquier tráfico que pase por ese segmento. El hecho que la tarjeta entre en estado promiscuo hace que, a nivel de capa de enlace, se almacenen todas las direcciones MAC que no eran destinadas a esta placa. Esto provoca que, pasado un tiempo, el switch alcance a conocer todas las direcciones existentes en la red, convirtiéndose en un hub. Este momento es cuando toda la información de la red es capturada por el sniffer.

Para evitar, o mitigar lo mas posible el problema de la “inundación” del switch, es necesario seguir alguno de los siguientes métodos:

- Puerto de seguridad

    - Permite especificar una dirección MAC para cada puerto o aprender un cierto número de direcciones MAC por puerto
    - Ante la detección de una MAC inválida, bloquear sólo la MAC ofensora o simplemente apagar el puerto.
- Tabla inteligente CAM
    - Nunca sobreescribir entradas existentes
    - Sólo entradas expiradas inactivas
    - Los hosts activos nunca serán sobreescritos
- Hablar primero
    - Requiere un host para enviar tráfico primero antes de recibir

Sniffers en Hubs

El escenario más básico lo encontramos en una red conectada mediante hub. En este caso posicionamos el sniffer en cualquier ranura o boca del hub y obtendremos, con la tarjeta en modo promíscuo, todo el tráfico de la red. Esto es así porque en un hub todos los paquetes son transmitidos a todos los hosts conectados en el mismo segmento de red.

Sniffers en Switchs

En este caso, a cada host conectado al switch, le llega solo el tráfico dirigido a él (unicast) y el broadcast. El tráfico dirigido a otros host no se lo verá. Existen distitnos métodos de sniffear utilizando un switch:

- ARP Poison: engañar a un determinado host diciéndole que la dirección MAC con quien se comunica sea otro host (C) distinto al que pretende comunicarse. De esta forma podemos redireccionar hacia (C) todo el tráfico que supuestamente debería ir de (A) –> (B).
- Colocar el sniffer en el gateway de salida a internet, o en un host firewall de varias tarjetas, indicar cuál de las interfaces nos interesa “olfatear”, de esta forma veremos algo más de tráfico que no sea el broadcast/multicast. Pero para ver todo el tráfico entre dos hosts las soluciones más eficaces son otras.
- Port Mirroring: consiste, básicamente, en copiar el tráfico entre dos puertos a un tercero (ubicación del host sniffer) del switch. El Port mirroring tiene el problema que multiplica la carga del switch.
- Conectar un hub a una de las salidas o puerto del switch y a este hub conectar el host sniffer (C) y uno de los host a capturar el tráfico (B). El otro host llamémosle (B) sigue en su ubicación del switch. De esta forma C puede ver el tráfico entre A y B. (B puede ser cualquier otro host conectado al switch o un servidor).
- Instalar otra interface de red en el host sniffer de forma que tenga dos interfaces de red. Una de las tarjetas la conectamos al switch y la otra a uno de los hosts a analizar. Esta opción se considera pasiva, pero necesita de configuración del host sniffer a nivel de interfaces de red para establecer el modo Bridge
- Network TAP o “Test Access Port” (Puerto de acceso de pruebas). Con este dispositivo podemos capturar el tráfico de una red conmutada de forma pasiva, es decir, no interfiere en el flujo o tráfico de nuestra red. Método más eficiente aunque también más costosa y quizás más incómoda.

Algunas de las buenas prácticas para lograr que los sniffers no logren ingresar a capa 2, y lograr su objetivo:

- Manejar switches de la manera más segura posible (ssh, oob, permit lists, etc.)
- Siempre usar un id VLAN dedicado para todos los puertos trunk
- Ser paranoico: no usar VLAN 1 para cualquier cosa
- Setear todos los puertos de usuario en modo NO trunk
- Utilizar puertos de seguridad en puertos de usuarios donde sea posible
- Usar selectivamente SNMP y tratar a los strings como root passwords
- Tener un plan para los problemas de seguridad ARP en la red
- Habilitar la mitigación de ataques STP (BPDU Guard, Root Guard)
- Usar VLANs privadas donde sea apropiado dividir dos redes
- Deshabilitar todos los puertos no utilizados y ponerlos en una VLAN no usada

- Considerar 802.1X como término medio

IPv6

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron ciertas funciones del IPv4, y las que se usan con poca frecuencia, o cuya relevancia no es significativa, se quitaron o se hicieron opcionales, agregándose nuevas características.

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Entre otras mejoras implementadas en IPv6, se pueden encontrar:

- Un espacio de direcciones superior, pasando de 32 bits a 128 bits
- Direcciones jerárquicas para reducir el tamaño de las tablas de encaminamiento en los encaminadores de la red troncal principal.
- Una cabecera simplificada, para que los encaminadores y pasarelas puedan procesar y encaminar los paquetes más rápidamente.
- Introducción de características mejoradas de seguridad e integridad de datos, incluyendo autenticación y cifrado.
- Una función de autoconfiguración, que permite a un computador obtener una dirección IP a través de la red sin intervención de un operador humano.
- Mejores garantías de calidad de servicio, mediante el tratamiento preferencial por parte de los encaminadores de los paquetes asociados a aplicaciones multimedia e interactivas con respecto a las aplicaciones tradicionales como correo electrónico.
- Soporte para computación móvil mediante el uso de la autoconfiguración, que permite obtener dinámicamente una dirección IP a través de la red.

Cabeceras de Expansión

Una de las principales virtudes que posee la utilización de IPv6 es que el formato del paquete que envía puede ir variando de acuerdo a la información opcional que permite transmitir. Esto es posible a través de la utilización de **cabeceras de expansión**. Los campos de opciones se codifican utilizando un formato denominado TLV (Type-Length-Value). Los campos tipo y longitud están formados por bytes que indican, respectivamente, el tipo de opción y su longitud. El valor de la opción está contenido en los bytes subsiguientes, tantos como se indican en el campo longitud. Según la RFC 2460 estas cabeceras pueden ser:

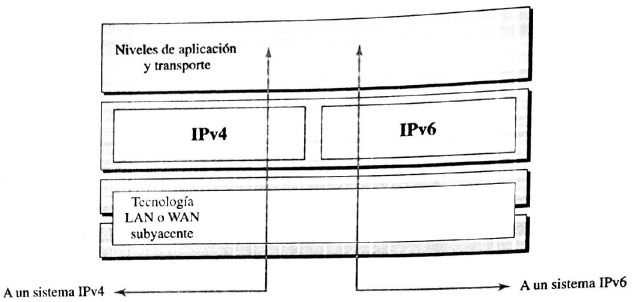
- **Opciones de salto a salto**: opciones especiales que necesitan procesamiento salto a salto
- **Opciones de Encaminamiento**: Se utiliza para dar una lista de uno o más nodos que deben estar en la ruta seguida por un paquete.
- **Opciones de Fragmentacion**: Se utiliza en caso de que el mensaje original enviado por el protocolo de transporte exceda la MTU del camino/ruta utilizado. El procedimiento de fragmentación se lleva a cabo en el computador fuente en lugar de realizarse en los encaminadores/pasarelas a lo largo del camino. Si el tamaño del mensaje (incluyendo la cabecera del protocolo de transporte) excede la MTU seleccionada el mensaje deberá fragmentarse en múltiples paquetes. Esta opcion permite el volver a armar el mensaje en el destino.
- **Autenticación y encapsulado de seguridad de los datos**: Son mecanismos utilizados para mejorar la seguridad de un mensaje durante su transferencia a través de una red. Su objetivo es permitir que el receptor de un mensaje pueda comprobar que el mensaje fue enviado verdaderamente por la dirección fuente especificada en la cabecera del paquete/datagrama y no por un impostor.
- **Opciones de Destino**: Se utilizan para transportar información que debe examinarse únicamente en el computador destinatario.

Interoperabilidad entre IPv4 e IPv6

Debido al enorme número de sistemas en internet, la transición de IPv4 a IPv6 no puede ocurrir de un momento al otro, de repente, sino que llevará un tiempo considerable que se logre migrar todos los dispositivos a esta nueva tecnología. Para comenzar el traspaso, se implementaron tres estrategias por parte de IETF (Internet Engineering Task Force): pila dual, túneles, y traducción de cabeceras.

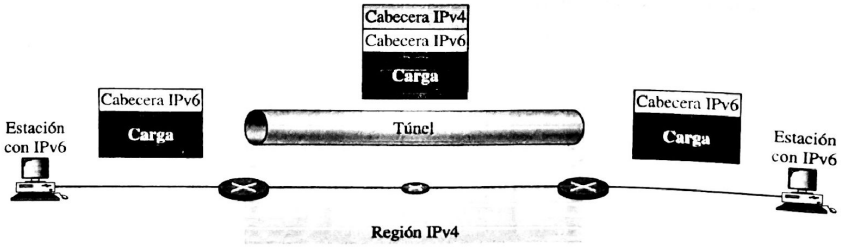
Pila Dual

El principal método para que un dispositivo logre migrar completamente de la versión 4 del protocolo de internet a la versión 6, es comenzar a operar con ambos en simultáneo. Es decir, poder tener una pila de protocolos de internet basados en versión 4, y versión 6.

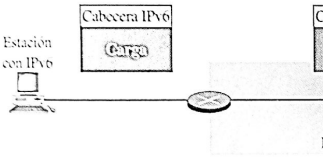


Para determinar qué versión utilizar cuando se envía un paquete a un destino, el emisor consulta el DNS. Si el DNS devuelve una dirección IPv4, el emisor envía un paquete acorde a dicha versión. En cambio, si la dirección corresponde a IPv6, el paquete es enviado de acuerdo a la pila de IPv6.

Túneles



Los túneles son utilizados cuando dos dispositivos que utilizan IPv6 quieren comunicarse entre sí, pero para hacerlo deben atravesar una región que usa IPv4. Para atravesarlo sin pérdida de información, el paquete IPv6 se encapsula en un paquete IPv4 cuando ingresa a la región, y se extra cuando la abandona. Debido a esta forma de operar es que el método recibe el nombre de túnel.



Traducción de Cabeceras

Este método es utilizado cuando se quieren comunicar un dispositivo que ya tiene implementado IPv6 con otro que no entiende esta nueva versión de IP. Para esto, es necesario realizar una conversión en el formato del paquete IPv6, ya que debe ser recibido en formato IPv4. Para ello, la cabecera debe cambiarse de acuerdo a un proceso de traducción de cabeceras.

Telefonía IP - VoIP

La **telefonía IP** es un conjunto de recursos que hace posible que la señal de voz viaje a través de internet empelando el protocolo IP. Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables solo por la telefonía convencional, como las redes PSTN (Public Switched Telephone Network, red telefónica pública conmutada).

Se debe hacer una distinción entre lo que es voz sobre IP (VoIP) y la telefonía IP. Lo primero implica el conjunto de normas, dispositivos y protocolos que permiten transmitir voz sobre protocolo IP, es decir, a la tecnología aplicada que da lugar a la comunicación. En cambio, la telefonía IP hace referencia al servicio disponible al público general, realizado con la tecnología VoIP.

El servicio de telefonía VoIP permite hacer y recibir llamadas por Internet a través de un adaptador de voz que convierte la señal análoga del teléfono tradicional en digital, para poder enviarla sobre la conexión de banda ancha. Este adaptador es un Gateway que se encarga de hacer de puente entre la red telefónica convencional y la red de telefonía IP.

Ventajas de la utilización de VoIP

La primer ventaja y la más importante es el costo de la utilización de telefonía IP: una llamada mediante telefonía VoIP es en la mayoría de los casos mucho más barata que su equivalente en telefonía convencional. Esto es básicamente debido a que se utiliza la misma red para la transmisión de datos y voz, la telefonía convencional tiene costos fijos que la telefonía IP no tiene, de ahí que esta es más barata. Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita, pero cuando se realiza una llamada de un teléfono IP a un teléfono convencional el costo corre a cargo del teléfono IP.

Con VoIP uno puede realizar una llamada desde cualquier lado que exista conectividad a internet. Dado que los teléfonos IP transmiten su información a través de internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión.

El desarrollo de códecs para VoIP (aLaw, G.729, G.723, etc.) ha permitido que la voz se codifique en paquetes de datos cada vez más pequeños. Esto deriva en que las comunicaciones de voz sobre IP requieran anchos de banda muy reducidos. Junto con el avance permanente de las conexiones ADSL en el mercado residencial, este tipo de comunicaciones están siendo muy populares para llamadas internacionales.

Desventajas de la utilización de VoIP

Dado que VoIP utiliza una conexión de red, la calidad del servicio se ve afectado por la calidad de esta línea de datos. Esto quiere decir que la calidad de una conexión VoIP se verá reducida por problemas como la alta latencia (tiempo de respuesta) o la pérdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VOIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

Además de la posible pérdida de calidad en la comunicación, VoIP no garantiza la seguridad en la misma, esto quiere decir, que la telefonía IP es susceptible a virus de distintos tipos, y hasta a hackers.

Pero uno de los principales puntos en contra que tiene la comunicación via IP es la llamada al servicio de emergencias del 911. Como se sabe, la telefonía IP utiliza direcciones IP para identificar un número telefónico determinado, el problema es que no existe forma de asociar una dirección IP a un área geográfica determinada. Como cada ubicación geográfica tiene un número de emergencias en particular no es posible hacer una relación entre un número telefónico y su correspondiente sección del 911. Para arreglar esto quizás en un futuro se podría incorporar información geográfica dentro de los paquetes de transmisión del VoIP.

Protocolos VoIP

H.323

El **Protocolo H.323**, se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en LANs (Redes de área local) pero ha evolucionado rápidamente para dirigir las crecientes necesidades de las redes de VoIP.

El Protocolo H.323 es un conjunto de normas para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable. Además, es independiente de la topología de la red y admite pasarelas, permitiendo usar más de un canal de cada tipo (voz, vídeo, datos) al mismo tiempo.

SIP

El **protocolo SIP** (Protocolo de Inicio de Sesiones) es un protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual.

Este protocolo permite el establecimiento de sesiones multimedia entre dos o más usuarios. Para hacerlo se vale del intercambio de mensajes entre las partes que quieren comunicarse.

Megaco/H.248

El protocolo H.248, también conocido como Megaco, define el mecanismo necesario de llamada para permitir a un controlador Media Gateway el control de puertas de enlace para soporte de llamadas de voz/fax entre redes IP

H.248 es un complemento a los protocolos H.323 y SIP: se utilizará el H.248 para controlar las Media Gateways y el H.323 o SIP para comunicarse con otro controlador Media Gateway.

MGCP

El protocolo MGCP, Media Gateway Control Protocol, fue diseñado inicialmente para simplificar en lo posible la comunicación con terminales como los teléfonos. MGCP utiliza un modelo centralizado (arquitectura cliente-servidor), de tal forma que un teléfono necesita conectarse a un controlador antes de conectarse con otro teléfono, así la comunicación no es directa.

Tiene tres componentes un MGC (Media Gateway Controller), uno o varios MG (Media Gateway) y uno o varios SG (Signaling Gateway), el primero también denominado dispositivo maestro controla al segundo también denominado esclavo.

SCCP

Skinny Client Control Protocol o SCCP es un protocolo propietario de control de terminal desarrollado originariamente Selsius Corporation, que actualmente es propiedad de Cisco. Se define como un conjunto de mensajes entre un cliente ligero y el CallManager. SCCP es un protocolo ligero que permite una comunicación eficiente con un sistema Cisco Call Manager. El Call Manager actúa como un Proxy de señalización para llamadas iniciadas a través de otros protocolos como H.323, SIP, RDSI o MGCP. El cliente Skinny usa TCP/IP para transmitir y recibir llamadas. Para el audio utiliza RTP, UDP e IP.

IAX

IAX (Inter-Asterisk Exchange protocol), es uno de los protocolos utilizado por Asterisk, que es un servidor PBX (central telefónica) de código abierto patrocinado por la empresa Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

El principal objetivo de IAX ha sido minimizar el ancho de banda utilizado en la transmisión de voz y vídeo a través de la red de Internet, con particular atención al control y a las llamadas de voz y proveyendo un soporte nativo para ser transparente a la NAT (traslación de direcciones de red). La estructura básica de IAX

se fundamenta en la multiplexación de la señalización y del flujo de datos sobre un simple puerto entre dos sistemas.

IAX2

El protocolo IAX2 fue creado por Mark Spencer para la señalización de VoIP en Asterisk. El protocolo crea sesiones internas y dichas sesiones pueden utilizar cualquier códec (Compresor-Descompresor de datos). que pueda transmitir voz o vídeo.

IAX2 es un protocolo robusto, lleno de novedades y muy simple en comparación con otros protocolos. Permite manejar una gran cantidad de códecs y un gran número de streams (flujos de datos), lo que significa que puede ser utilizado para transportar virtualmente cualquier tipo de dato. Esta capacidad lo hace muy útil para realizar videoconferencias o realizar presentaciones remotas.

IAX2 soporta Trunking (red), donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia o retardo adicional

Power over Ethernet (PoE):

Power over Ethernet es una tecnología sobre Ethernet que permite la alimentación eléctrica, junto a la transmisión de información a través de la infraestructura de la red LAN. Esta tecnología está normalizada por la IEEE como 802.3af.

Esta tecnología se basa en enviar y recibir datos, a la vez que se suministra una corriente eléctrica hacia dispositivos de bajo voltaje como cámaras de vigilancia, Wireless LAN Access Point y voz en teléfonos IP. Esto permite suministrar electricidad a lugares de difícil alcance o sin instalaciones eléctrica cercana, quitando así el inconveniente de agregar nuevas instalaciones e implementando a Ethernet como un medio de conexión eléctrica además de traspasos de datos.

En el proceso de configuración cuando se hace una conexión PoE, el dispositivo conectado le comunica al dispositivo encargado de configurar la conexión la energía que requiere para funcionar. Esto determina la clase de PoE que utilizara, determinadas por la siguiente tabla

La clase 1 llega hasta un máximo de 3.84W de suministro de energía, esta clase se suele usar para teléfonos IP. La clase 2, con un máximo de 6.49W, es más utilizada para la configuración de cámaras de seguridad IP. Por último, la clase 3 y/o 0 se utilizan para puntos de acceso Wireless.

Ventajas de PoE

- Conectividad: PoE no necesita cables especiales para su conexión, puede trabajar con los cables estándar CAT-5 a CAT-7A de 2 pares (low power) o 4 pares (high power), y pueden ser shielded o unshielded.
- Costos de instalación: La utilización de PoE reduce la necesidad de una instalación eléctrica en lugares remotos, lo que lleva a una reducción de aproximadamente 1000USD por cada dispositivo conectado por PoE.
- Backup: Al desligarse de la conexión eléctrica convencional, PoE puede trabajar de forma continua aun cuando la corriente eléctrica se encuentra con interrupciones.
- Manejo de energía: PoE permite determinar que dispositivos pueden estar siendo suministrados o no, reduciendo su consumo en momentos de poco uso, o priorizándolos para propósitos de seguridad.

Conectividad

El estándar IEEE 802.3af del 2003 especifica la forma de conectividad PoE. Esta no se realiza de forma directa al dispositivo, sino que existe un Power Supplying Equipment (PSE) que suele ser un switch, con dos metodologías diferentes, según la instalación que se está desarrollando. Los dispositivos a ser suministrados aceptan cualquiera de las dos metodologías.

La metodología END-SPAN, se basa en un switch PoE, conectado directamente a la fuente de alimentación, ya sea corriente directa o batería UPS. En esta metodología se suele utilizar el modo de transición compartido. Esta metodología se usa para realizar toda una instalación enfocada en PoE.

Desde el switch PoE, se conectan los dispositivos que van a ser suministrados directamente a través de Ethernet. Una vez conectado, el switch detectara si los dispositivos son compatibles con PoE y podrá transmitir energía automáticamente.

La segunda metodología es conocida como MID-SPAN, en esta el switch PoE se encuentra en medio de la conectividad. Se suele utilizar como una actualización a una red LAN ya existente donde ya hay un switch que conduce datos a diferentes DTE, y provee una solución versátil solo algunos puertos PoE son necesarios.

Se trata de parchar la red con un switch PoE, conocido como PoE Inyector. Este funciona como un switch end-span pero que a su vez transmite y recibe datos del switch principal de la red que se está actualizando.

Power pver Data Line (PoDL)

A la hora de usar Ethernet en espacios como autos o maquinaria industrial pequeña se generan varios problemas. En primer lugar, y el más simple, es el hecho de que la cantidad de cables genera un gran peso y ocupa demasiado espacio como para poder ser usado en esos lugares. Por otro lado está que los costos de colocar este cableado en un auto son altos.

Por estos motivos se buscó una nueva forma de utilizar Ethernet usando solamente un par trenzado de cobre, lo que permitiría reducir peso, espacio y costos. Para esto se creó PoDL, que es una tecnología estandarizada sobre Ethernet, que permite una transferencia en full dúplex utilizando un solo para trenzado de cobre. Lo que se hace es enviar la energía necesaria, como así también la información, por el mismo par. Para esto se utiliza filtros pasa alto y pasa bajo para poder separar lo que es energía (frecuencias más bajas) de lo que es información (frecuencias más altas).

Tecnologías sobre Ethernet

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbit/s	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbit/s	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbit/s	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100 Mbit/s	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100 Mbit/s	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100 Mbit/s	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000 Mbit/s	(categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000 Mbit/s	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000 Mbit/s	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)