Administración avanzada de redes

TCP/IP

Javier Carmona Murillo
David Cortés Polo
Manuel Domínguez Dorado
Alfonso Gazo Cervero
José Luis González Sánchez
Francisco Javier Rodríguez Pérez

ISBN: 978-84-695-2037-6

Administración avanzada de redes TCP/IP

Javier Carmona Murillo
David Cortés Polo
Manuel Domínguez Dorado
Alfonso Gazo Cervero
José Luis González Sánchez
Francisco Javier Rodríguez Pérez

1ª edición: Enero de 2012
ISBN13: 978-84-695-2037-6

Objetivos del libro

•La familia de protocolos TCP/IP es la base de funcionamiento de Internet y, por ello, cualquiera de los actuales servicios de Internet tiene su correspondencia con uno o varios protocolos de la pila TCP/IP.

• Por esto, la pila es soportada actualmente en todos los sistemas operativos del mercado, lo que requiere un conocimiento profundo de la misma si se desea obtener el mejor rendimiento de los sistemas conectados a la Red.

• El objetivo general del libro es presentar, conocer, comprender, configurar, utilizar y avaluar los protocolos más importantes de la familia de protocolos de comunicaciones que da soporte a los servicios y al funcionamiento de Internet.


Nº 1

Administración Avanzada de Redes TCP/IP

Índice


Nº 2

Temario

7) Protocolos para la provisión de QoS (RSVP, IntServ, DiffServ, MPLS, etc.).

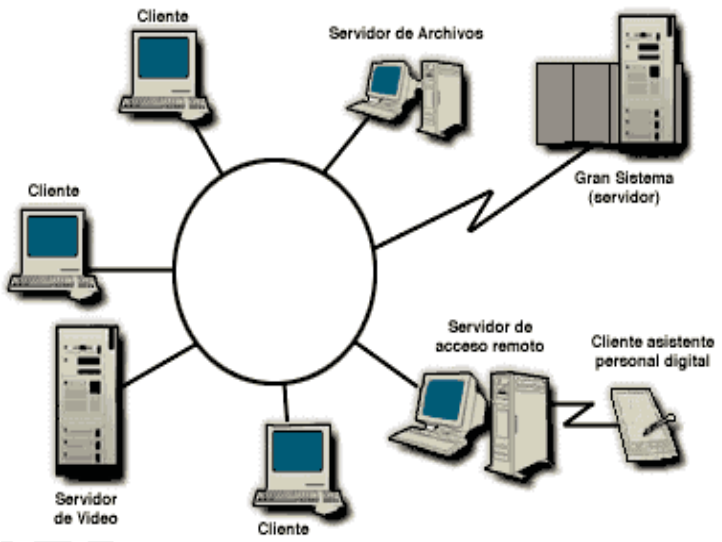
8) Movilidad IP.

9) Seguridad en redes IP.

10) Miscelánea: DHCP, HTTP, P2P, etc.

11) Administración y mantenimiento.

1. Introducción a la familia de protocolos TCP/IP



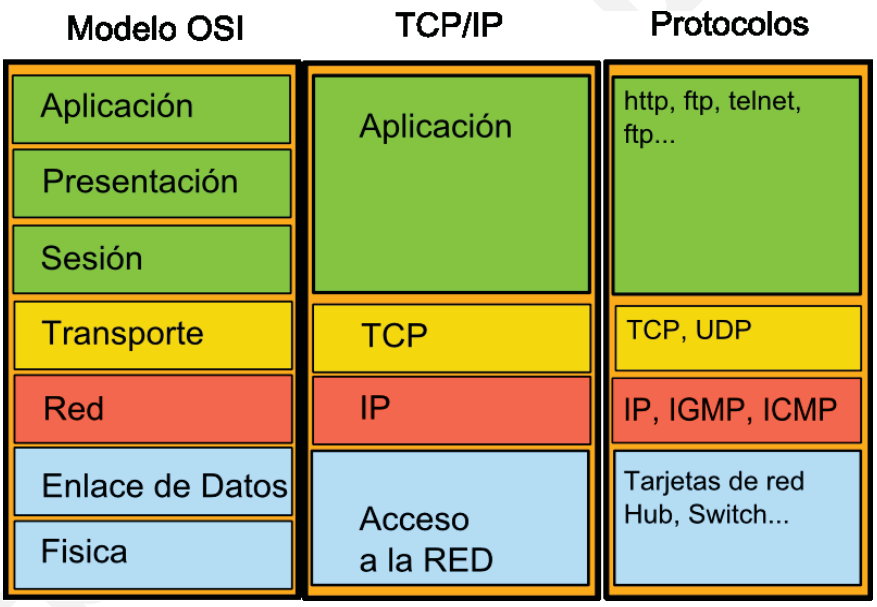
1) Introducción a la familia de protocolos TCP/IP

Objetivos

- Introducir la pila TCP/IP.
- Funciones y cabecera IPv4.
- Funciones y cabecera TCP.

Administración Avanzada de Redes TCP/IP

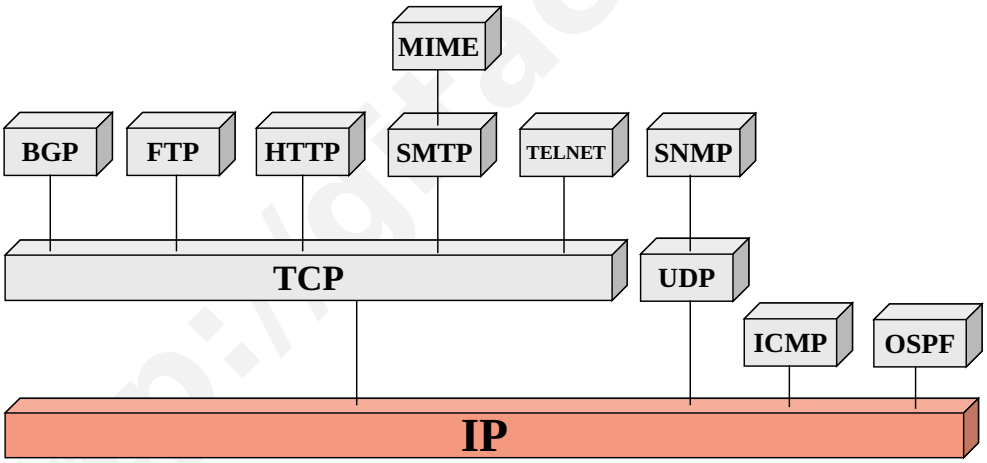
1) Introducción a la familia de protocolos TCP/IP



1) Introducción a la familia de protocolos TCP/IP

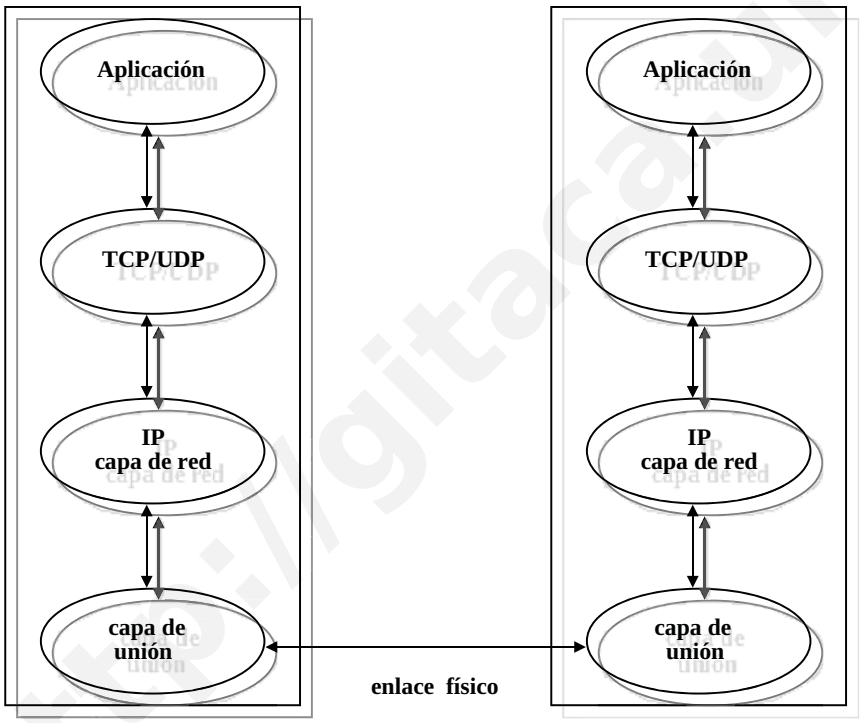
BGP: Border Gateway Protocol
FTP : File Transfer Protocol
HTTP: Hypertext Transfer Protocol
ICMP: Internet Control Message Protocol
IP: Internet Protocol
OSPF: Open Shortest Path First

MIME: Multi-Purpose Internet Mail Extensions
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
UDP: User Datagram Protocol
PIM, DVMRP, MOSPF, Gopher, NNTP, etc....

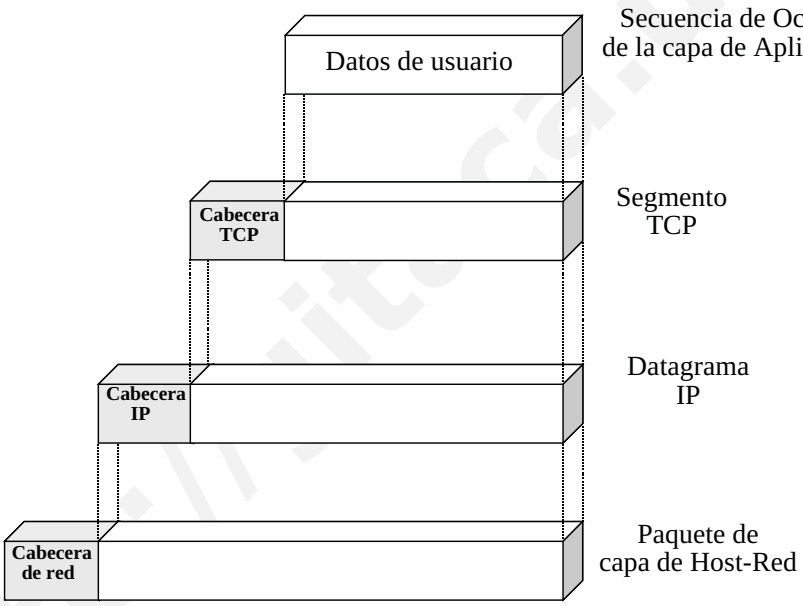


Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP



1) Introducción a la familia de protocolos TCP/IP



Tipos de paquetes de la arquitectura TCP/IP

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

- Las redes interconectadas entre sí son muy diferentes por lo que el nivel de red IP debe adaptarse a esa diversidad.
- La manera más flexible de adaptarse es introduciendo una interfaz software que es proporcionada, normalmente, por el sistema operativo.
- Además, lo que en TCP/IP pura se llama Nivel de Acceso, en la mayoría de las redes existentes se divide en dos niveles: Nivel Físico y Nivel de Enlace. También puede haber subniveles dentro de ellos.
- Una arquitectura de un Sistema Final conectado a una red (cualquiera de las existentes) que además tenga acceso a y desde otras redes podría ser…

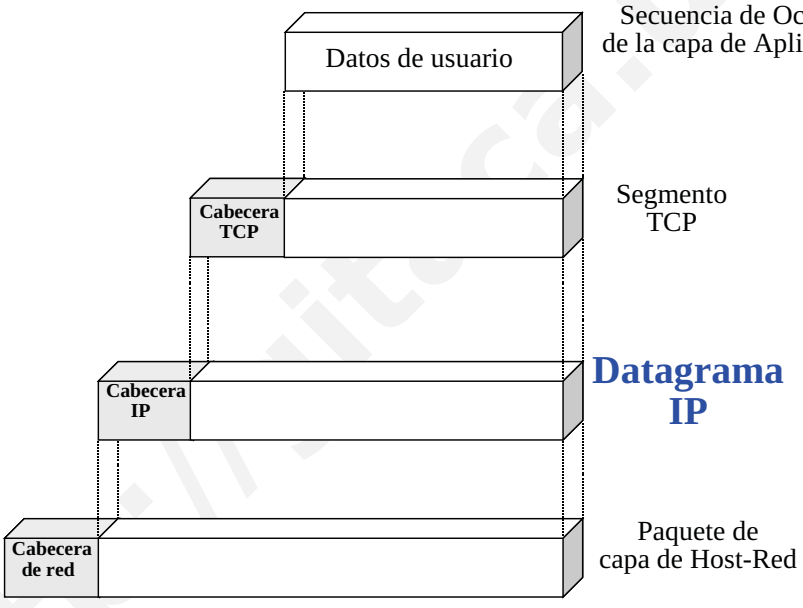
1) Introducción a la familia de protocolos TCP/IP

NIVEL DE APLICACIÓN
INTERFAZ DE PROG. DE APLICACONES (API)
NIVEL DE TRANSPORTE (TCP o UDP)
NIVEL DE RED (IP y protocolos asociados)
INTERFAZ DE CONTROLADOR DE RED
NIVEL DE ENLACE
NIVEL FÍSICO

Arquitectura TCP/IP genérica

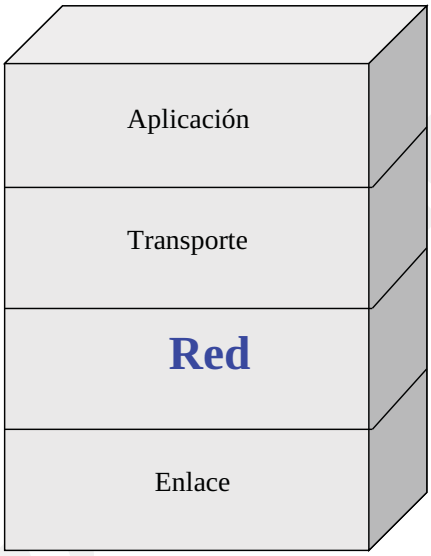
Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP



Tipos de paquetes de la arquitectura TCP/IP

1) Introducción a la familia de protocolos TCP/IP

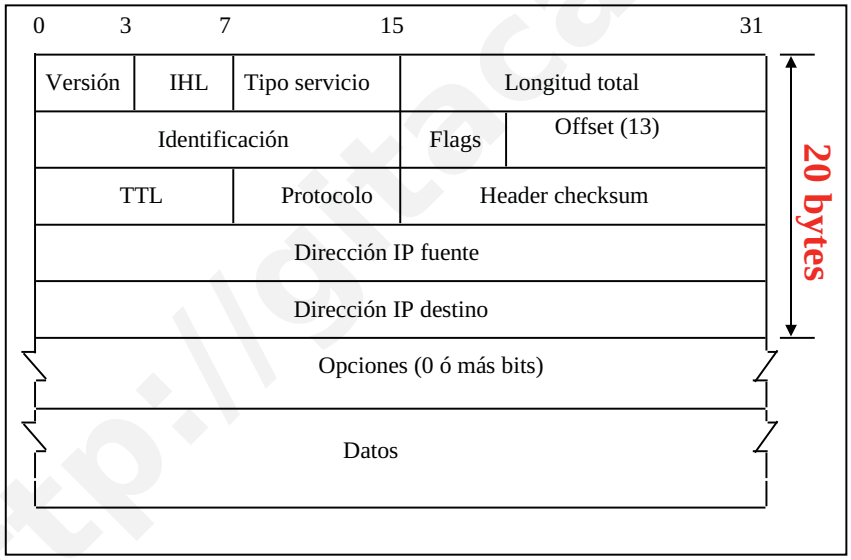


Relación de protocolos TCP/IP con las capas del modelo de referencia

Administración Avanzada de Redes TCP/IP

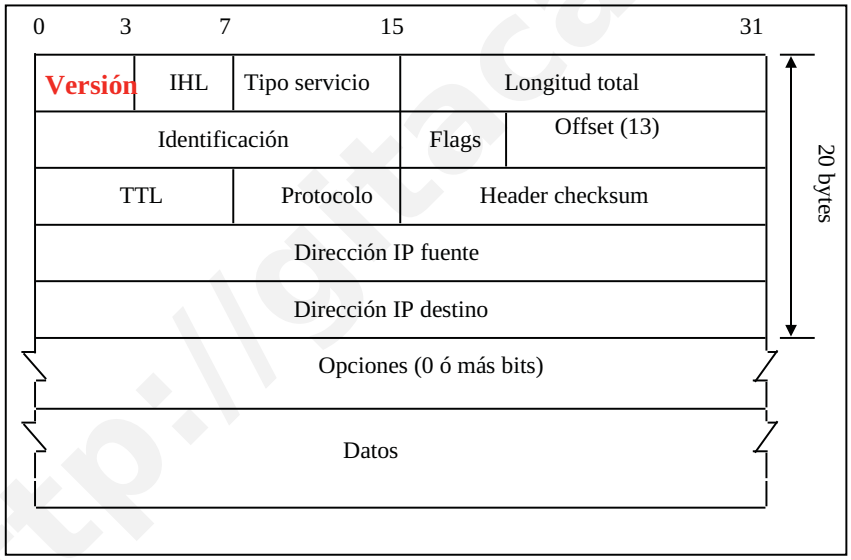
1) Introducción a la familia de protocolos TCP/IP

Datagrama IP: cabecera (parte fija de 20 octetos + parte opcional de longitud variable) y datos variable.



1) Introducción a la familia de protocolos TCP/IP

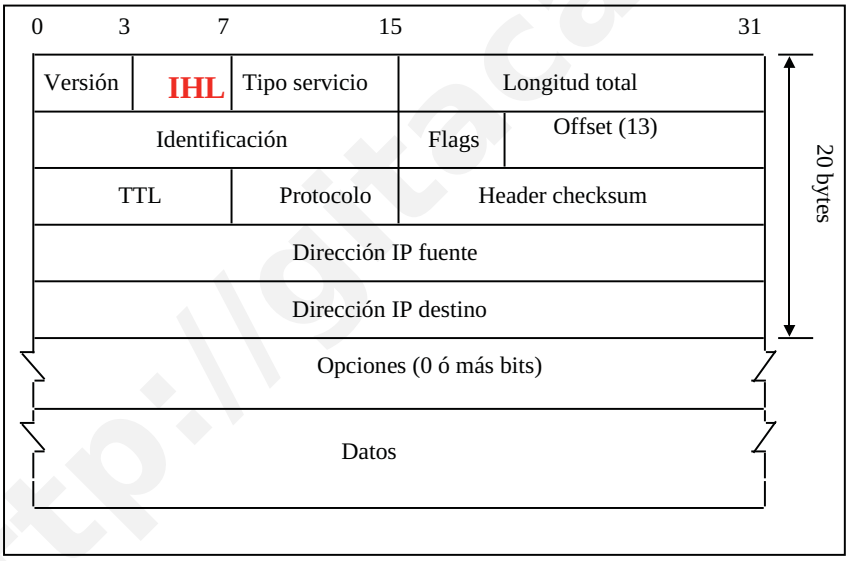
Versión: de IP al que pertenece el datagrama (4 bits).



Nº 15

Administración Avanzada de Redes TCP/IP

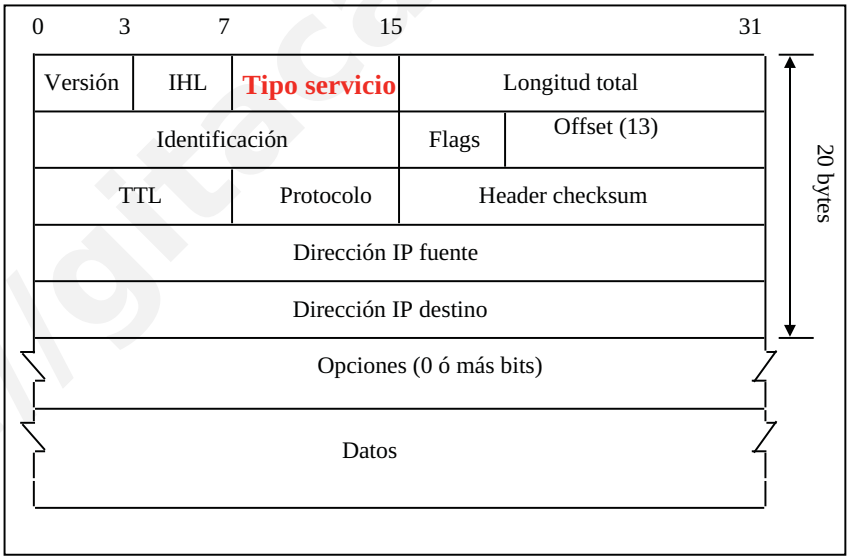
IHL (IP Header Length): Longitud máxima de la cabecera en palabras de 32 bits. (4 bits). Valor mínimo de IHL= ¿.?; Valor máximo=15 * 4 = 60; por tanto, campo opciones puede tener una longitud máxima de 40 bytes. Si se incluye una o más opciones hay que rellenar la cabecera para que tenga un múltiplo de palabras de 32 bits.



Nº 16

ToS (Type of Service): para que el nodo indique el tipo de servicio que desea. Combinaciones de fiabilidad y velocidad (8 bits):

- 3 bits: campo de precedencia (0= prioridad normal y 7 = control de red).
- 4 indicadores: D(mínimo delay), T(máximo Troughtput), R(máxima fiabilidad), C(mínimo coste).
- 1 bit reservado uso futuro.



Nº 17

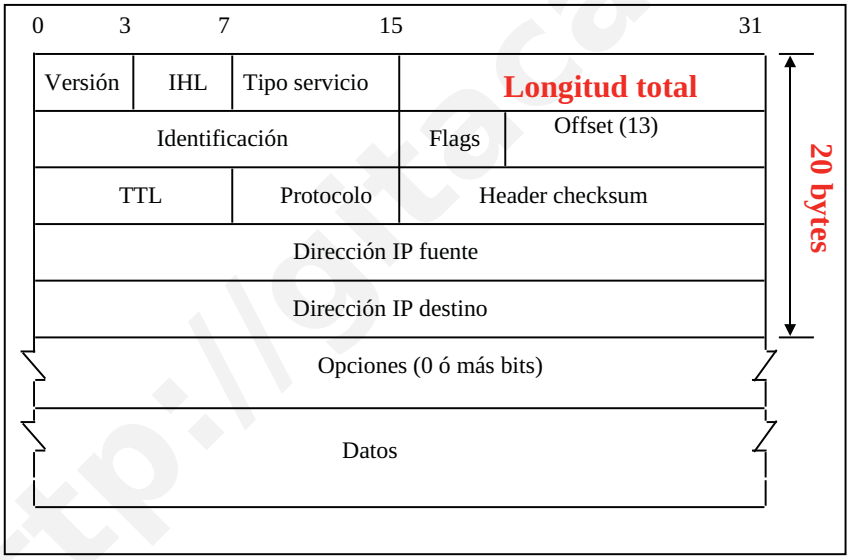
Administración Avanzada de Redes TCP/IP

ToS (Type of Service): para que el nodo indique el tipo de servicio que desea. Combinaciones de fiabilidad y velocidad (8 bits):

Aplicación	Mínimo retardo	Máximo Throughput	Máxima fiabilidad	Mínimo coste monetario	Valor Hex
Telnet/Rlogin	1	0	0	0	0x10
FTP					
Control	1	0	0	0	0x10
datos	0	1	0	0	0x08
SMTP					
Fase comando	1	0	0	0	0x10
Fase datos	0	1	0	0	0x08
DNS					
Query UDP	1	0	0	0	0x10
Query TCP	0	0	0	0	0x00
zona transfer	0	1	0	0	0x08
SNMP	0	0	1	0	0x04

Nº 18

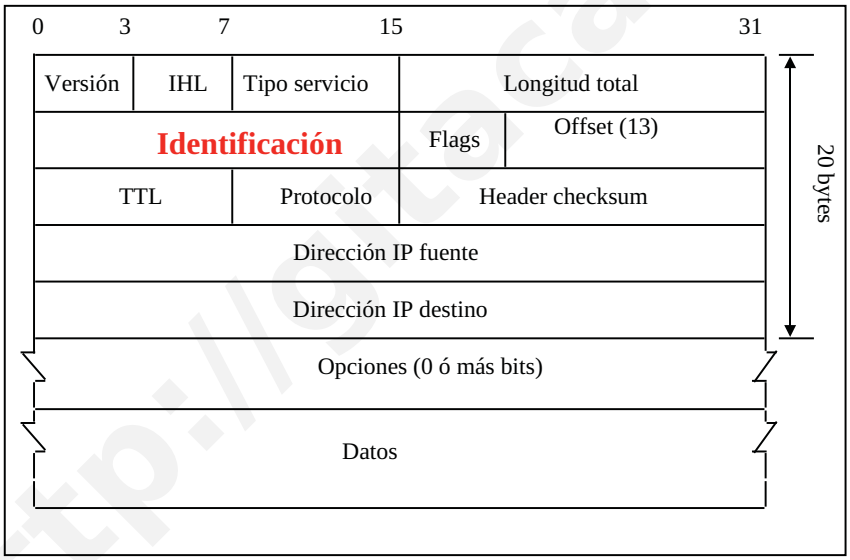
Longitud total: total del datagrama completo (cabecera + datos). (16 bits).
Máximo= 65.535 = 2^{16}-1 bytes y Mínimo=48 bytes.
El tamaño lo limita la tecnología de red y el tipo de ordenador (buffers).
Norma: todos los hosts deben ser capaces de aceptar datagramas de hasta 576 octetos.



Nº 19

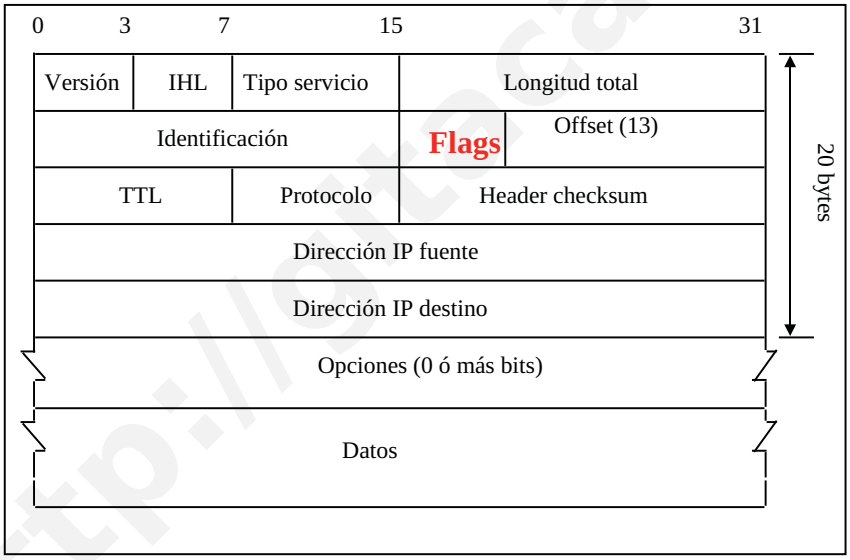
Administración Avanzada de Redes TCP/IP

Identificación: para determinar en el destino a qué datagrama pertenece un fragmento de un datagrama que puede haber sido fragmentado por la red.



Nº 20

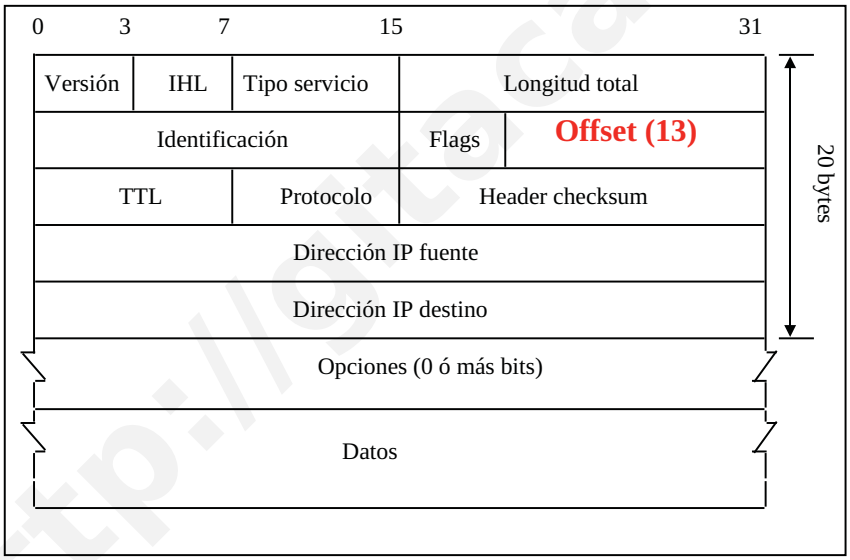
3 flags: - 1 bit no usado.
- bit **DF** (*Don't Fragment*) para que los routers no fragmenten un datagrama.
- bit **MF** (*More fragments*) activado en todos los fragmentos (menos el último) de un datagrama.



Nº 21

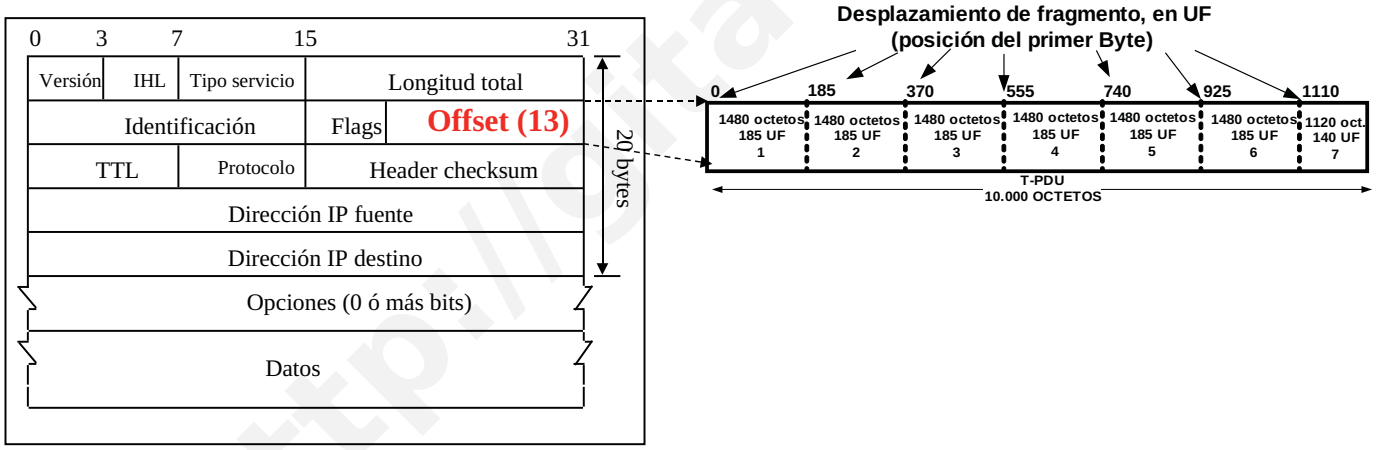
Administración Avanzada de Redes TCP/IP

Desplazamiento del fragmento: (13 bits) 8.192 fragmentos por datagrama como máximo. Actúa a modo de "puntero" para mantener la secuencia de los fragmentos de un datagrama que ha sido fragmentado.

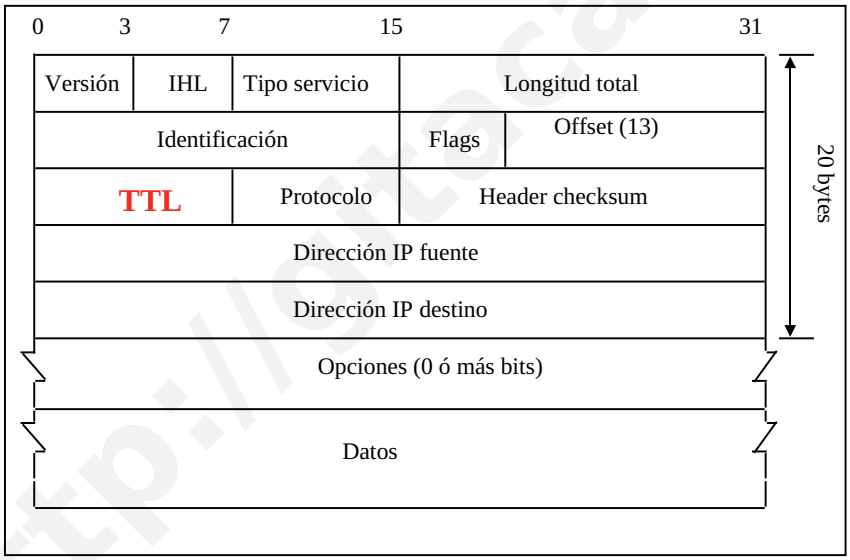


Nº 22

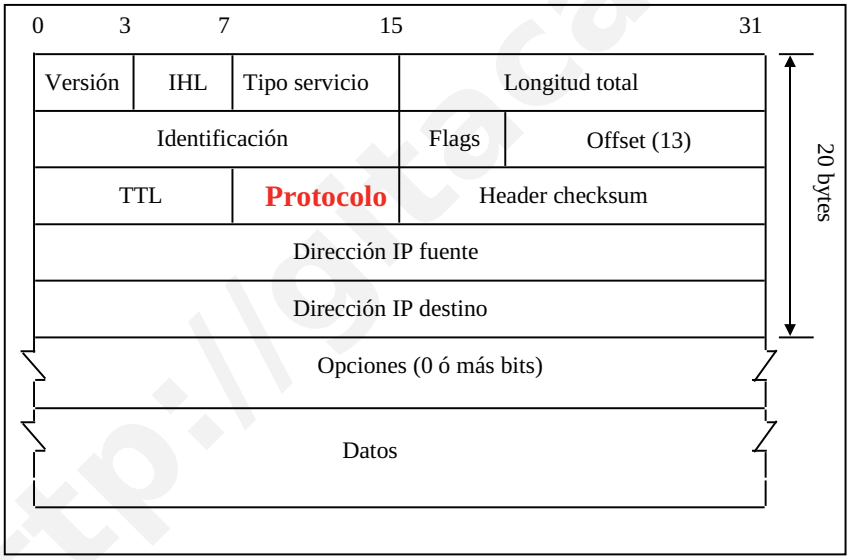
Desplazamiento del fragmento: (13 bits) Indica la porción de la T-PDU original que ha sido fragmentada, que va en el datagrama actual. Esta porción se mide en Unidades de Fragmento Elementales, que equivale cada una a 8 bytes. Todos los datagramas resultantes de una fragmentación, excepto el último, deben tener una longitud que sea múltiplo de 8 bytes. Indica la posición del primer byte del campo de datos de usuario de cada datagrama en UF y en relación con la T-PDU (segmento) original.



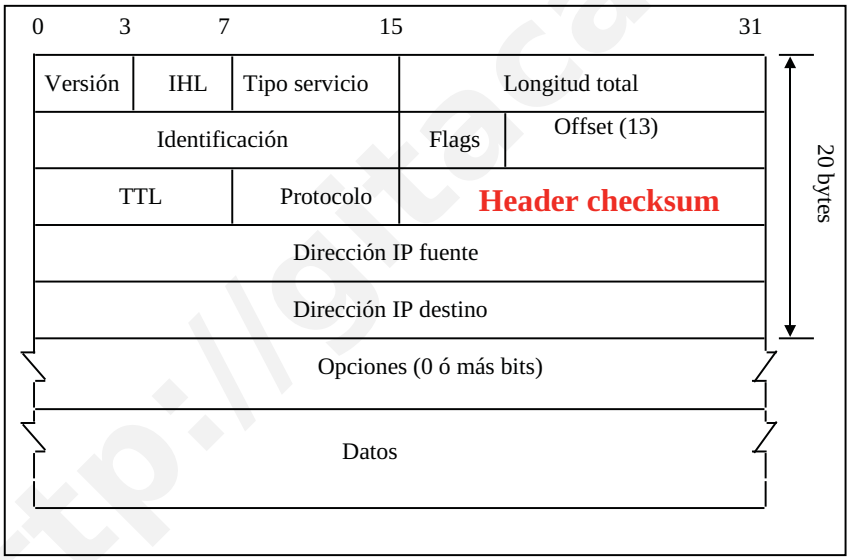
TTL (Time To Live): máximo número de saltos (routers) que puede atravesar un datagrama concreto antes de ser "tirado" por la red. Cada router decrementa en uno el valor TTL de salida del datagrama hasta llegar a 0 en que es desechado.



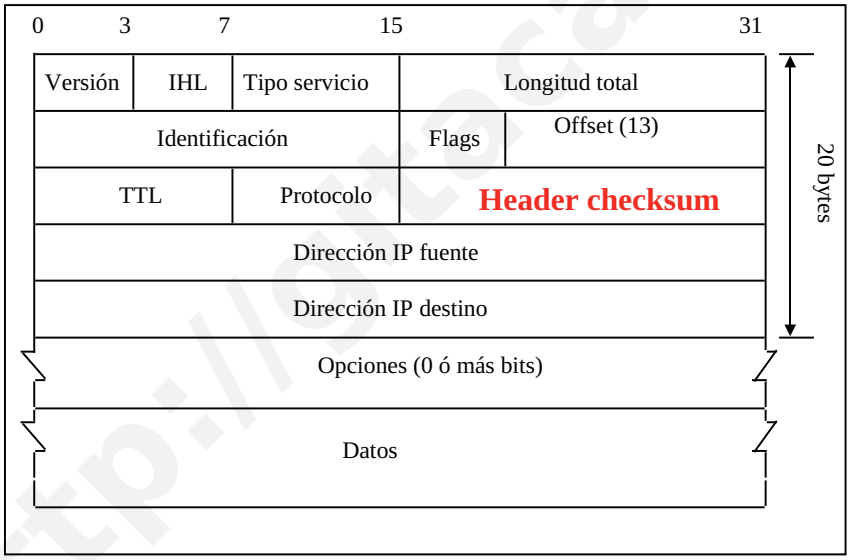
Protocolo: indica la capa de transporte (TCP, UDP) a la que debe entregarse el datagrama desde la capa de red.



Checksum: CRC que verifica sólo la cabecera para localizar errores. Método simple para detectar algunos errores. Este campo se rellena sumando en complemento a uno las palabras de 16 bits del encabezado del datagrama. Este resultado (de 16 bits) se complementa a su vez a uno y se coloca en este campo.



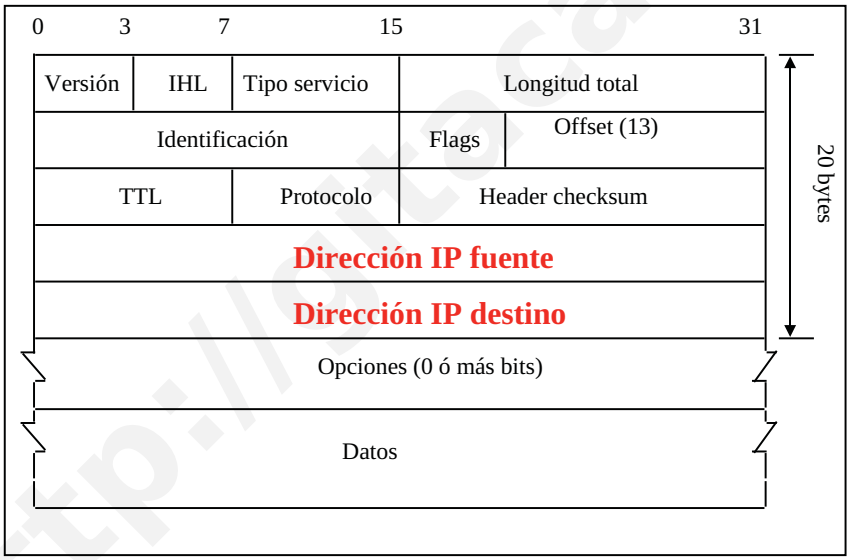
Checksum: El receptor hace la suma de la misma manera que el emisor, con palabras de 16 bits, incluyendo además los 16 bits de este campo. El resultado debe ser todo unos, ya que si a un número binario cualquiera le sumamos su complemento a uno el resultado es todo unos (o bien cero en C-1, que es lo mismo). Si no es así, ha habido un error por lo que el datagrama se descarta. Similar al Checksum en OSI.



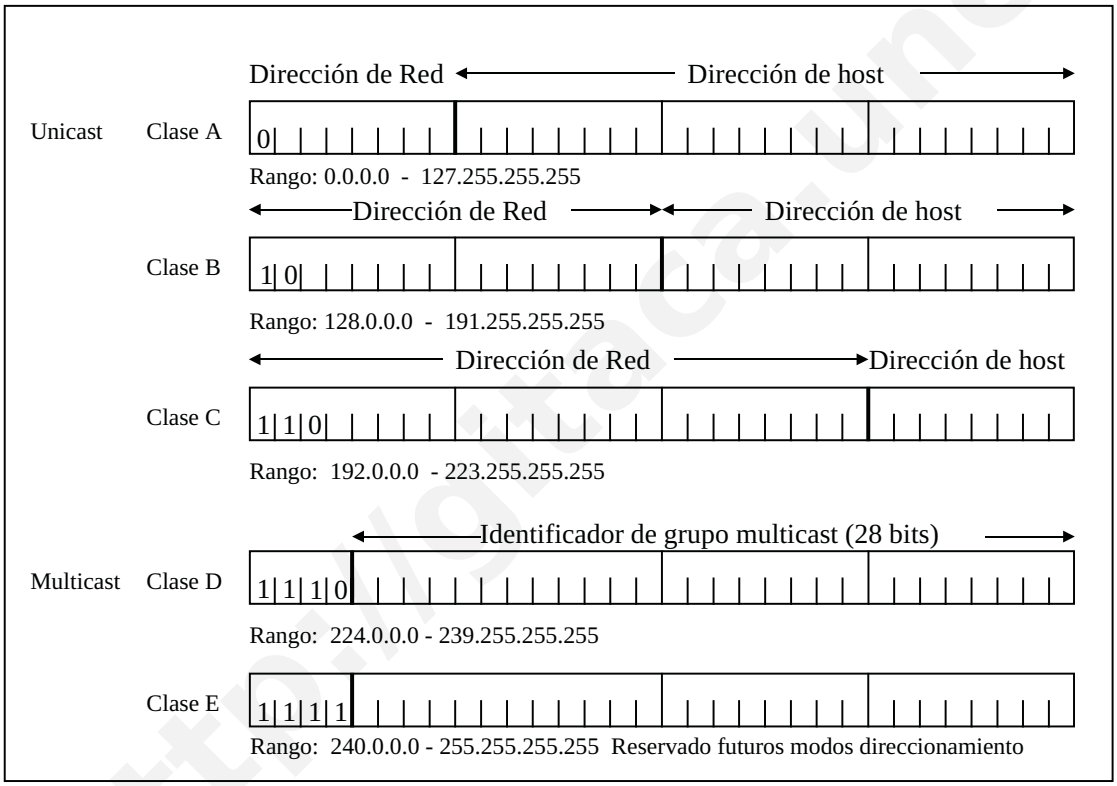
Nº 27

Administración Avanzada de Redes TCP/IP

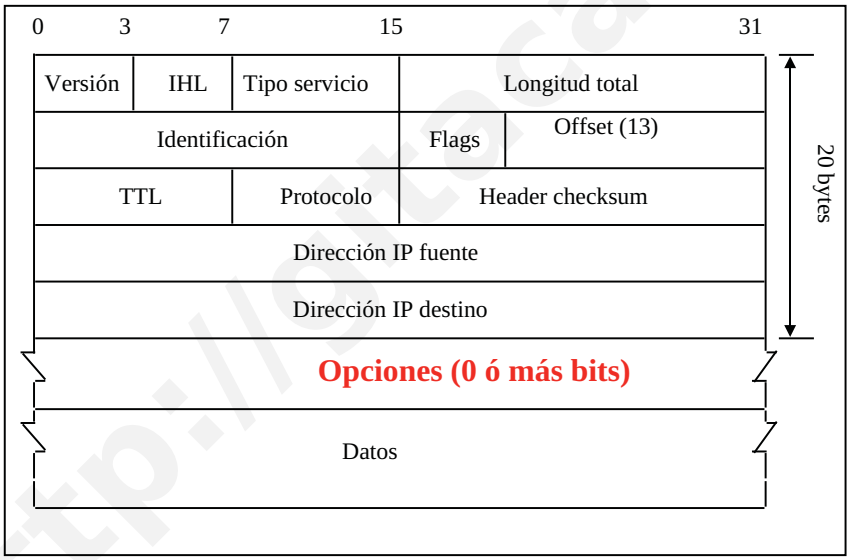
Dirección IP fuente y destino: campos de 32 bits cada uno de ellos que se estructuran según lo siguiente:



Nº 28



Opciones (5 bytes): Seguridad, ruta estricta desde origen, ruta libre, registrar ruta, marca de tiempo.



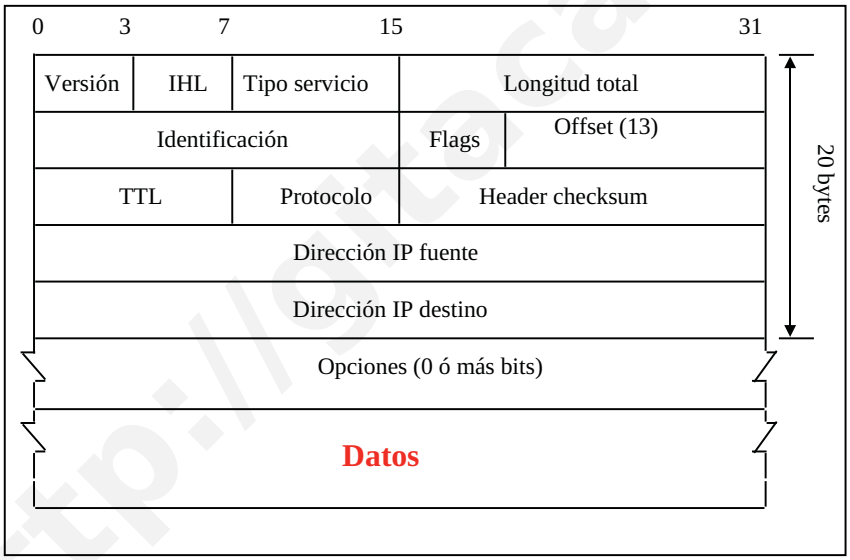
Opciones (5 bytes): Estas opciones raramente se usan pues no todos los nodos y routers lo soportan. Este campo siempre acaba con un redondeo a 32 bits. Se añaden bytes de relleno con valor a 0 si es necesario. Esto asegura que la cabecera IP es un múltiplo de 32 bits (como requiere el campo *header length*).

Opción	Descripción
Seguridad	Especifica el grado de secreto del datagrama
Encaminamiento estricto desde el origen	Se indica la ruta completa a seguir
Encaminamiento libre desde el origen	Da una lista de los routers que no deben evitarse
Registrar ruta	Cada router por donde pasa el datagrama agrega su dirección en este campo
Marca de tiempo	Además de su dirección el router agrega una marca de tiempo, que tiene como objetivo detectar fallos en los algoritmos de encaminamiento

Nº 31

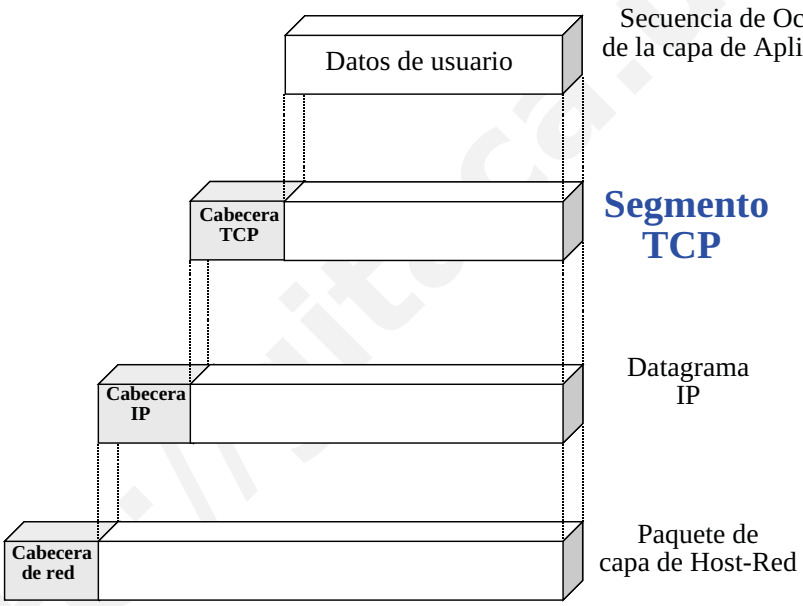
Administración Avanzada de Redes TCP/IP

Datos: Tamaño variable.



Nº 32

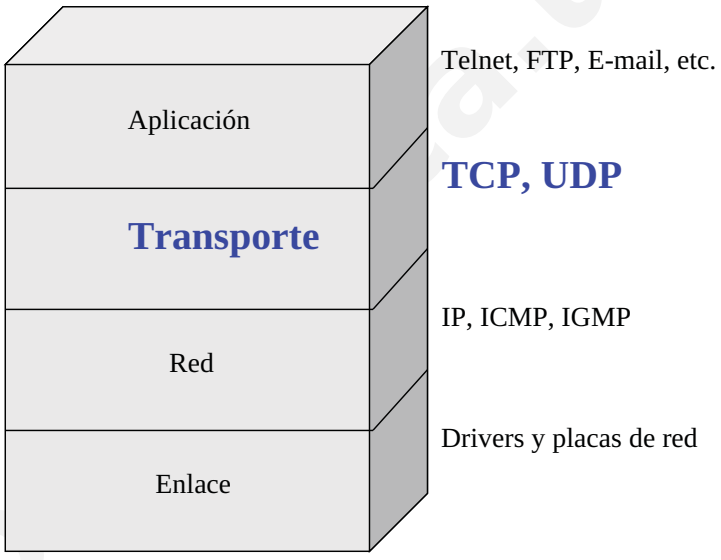
1) Introducción a la familia de protocolos TCP/IP



Tipos de paquetes de la arquitectura TCP/IP

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

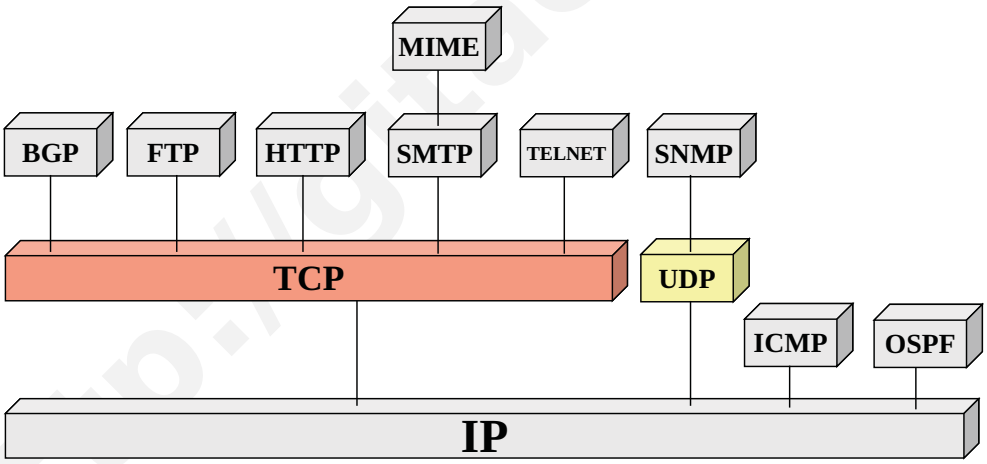


Relación de protocolos TCP/IP con las capas del modelo de referencia

1) Introducción a la familia de protocolos TCP/IP

BGP: Border Gateway Protocol
FTP : File Transfer Protocol
HTTP: Hypertext Transfer Protocol
ICMP: Internet Control Message Protocol
IP: Internet Protocol
OSPF: Open Shortest Path First

MIME: Multi-Purpose Internet Mail Extensions
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
UDP: User Datagram Protocol
PIM, DVMRP, MOSPF, Gopher, NNTP, etc....



Protocolos más importantes de la familia TCP/IP

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

- La capa superior a IP conocida usualmente como capa de transporte.

- TCP (Transmission Control Protocol):
  - Protocolo extremo-extremo.
  - Fiable.
  - Orientado a conexión.
  - Control de flujo para evitar que emisor rápido congestione receptores más lentos.
  - Para aplicaciones que requieren más fiabilidad que rapidez (datos).

- UDP (User Datagram Protocol):
  - Protocolo sin conexión.
  - No fiable.
  - No necesita control de flujo.
  - Para aplicaciones que prefieren la rapidez a la precisión (audio y video).

1) Introducción a la familia de protocolos TCP/IP

- Internet: diversas topologías, tecnologías, anchos de banda, tamaños de paquete, retardos, etc.
- TCP diseñado para adaptarse dinámicamente a las diversas propiedades de la Red.
- Definición formal en RFC 793. RFC 1122 corrige diversos errores.
- RFC 1323 extensiones de TCP.
- Emisor y receptor necesitan puntos terminales (*sockets*).
- Cada *socket* tiene un número: @IP del host + Nº port (nº de 16 bits local al host).
- Para lograr el servicio TCP debe crearse una conexión explícita entre un *socket* del nodo emisor y otro *socket* del nodo receptor.

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

Primitivas	Significado
socket(enchufar)	Crea un punto terminal de comunicación
bind (ligar)	Conecta una dirección local a un socket
listen (escuchar)	Anuncia disponibilidad para aceptar conexiones expresando tamaño de cola
accept (aceptar)	Bloquea al invocador hasta la llegada de un intento de conexión
connect (conectar)	Intenta establecer una conexión activamente
send (enviar)	Envía datos a través de la conexión
receive (recibir)	Recibe datos a través de la conexión
close (cerrar)	Libera la conexión

Primitivas de *sockets* de TCP

1) Introducción a la familia de protocolos TCP/IP

- Un *socket* puede recibir una o varias conexiones al mismo tiempo.
- Las conexiones se identifican con (*socket1*, *socket2*) sin ningún otro identificador ni circuito virtual.
- Todas las conexiones TCP son:
  - Dúplex integral: el tráfico puede ir en ambos sentidos a un tiempo.
  - Extremo a extremo: cada conexión tiene exactamente dos puntos terminales (TCP no reconoce difusión ni multitransmisión).
- Una conexión TCP es una corriente de bytes y no una corriente de mensajes, por lo que los límites de los mensajes no se conservan extremo a extremo y los receptores no pueden detectar las unidades de transmisión del origen.
- Los datos pueden ser enviados inmediatamente (PUSH) o almacenados en buffers.

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

- El servicio TCP permite también definir datos urgentes (URGENT).
- Cada conjunto de bytes de una conexión tiene su propio nº de secuencia de 32 bits.
- Las entidades transmisoras y receptoras TCP intercambian datos en forma de segmentos. Pueden emitir y recibir datos a la vez.
- La transmisión de datos de nivel de transporte presenta tres fases:
  - Establecimiento de conexión.
  - Intercambio de datos.
  - Liberación de conexión.

1) Introducción a la familia de protocolos TCP/IP

- Un segmento TCP es un paquete de datos formado por:
  - una cabecera de tamaño fijo de 20 bytes.
  - una parte opcional de tamaño variable.
  - cero o más bytes de datos.
- El protocolo TCP decide el tamaño de los segmentos con dos límites:
  - Cada segmento TCP (incluida cabecera) debe caber en los 65.535 bytes de IP.
  - Cada red tiene su MTU y cada segmento debe caber en una MTU. La MTU define el límite superior del tamaño del segmento.
- Un segmento demasiado grande es fragmentado por los routers frontera (*overhead*).

Administración Avanzada de Redes TCP/IP

1) Introducción a la familia de protocolos TCP/IP

PROTOCOLO BÁSICO: VENTANA DESLIZANTE

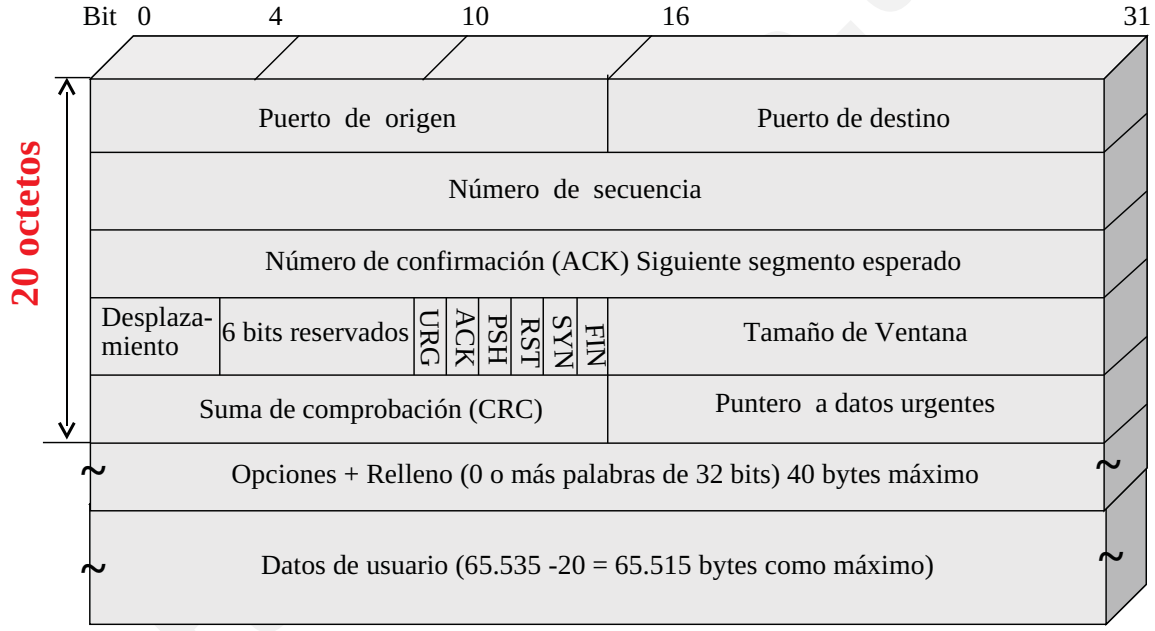
- Emisor envía un segmento e inicia un temporizador. La cabecera de cualquier segmento de TCP contiene el Nº de secuencia del primer octeto de los datos en el segmento.
- Cuando receptor recibe el segmento, el TCP del receptor devuelve un segmento (con datos o sin ellos) con Nº de ACK igual al siguiente Nº de secuencia que espera recibir.
- Si temporizador del emisor expira antes de la recepción del ACK, el transmisor envía el segmento de nuevo (ACK + con retransmisión).
- Garantiza la entrega fiable y ordenada de datos. Fuerza control de flujo entre emisor y receptor.

1) Introducción a la familia de protocolos TCP/IP

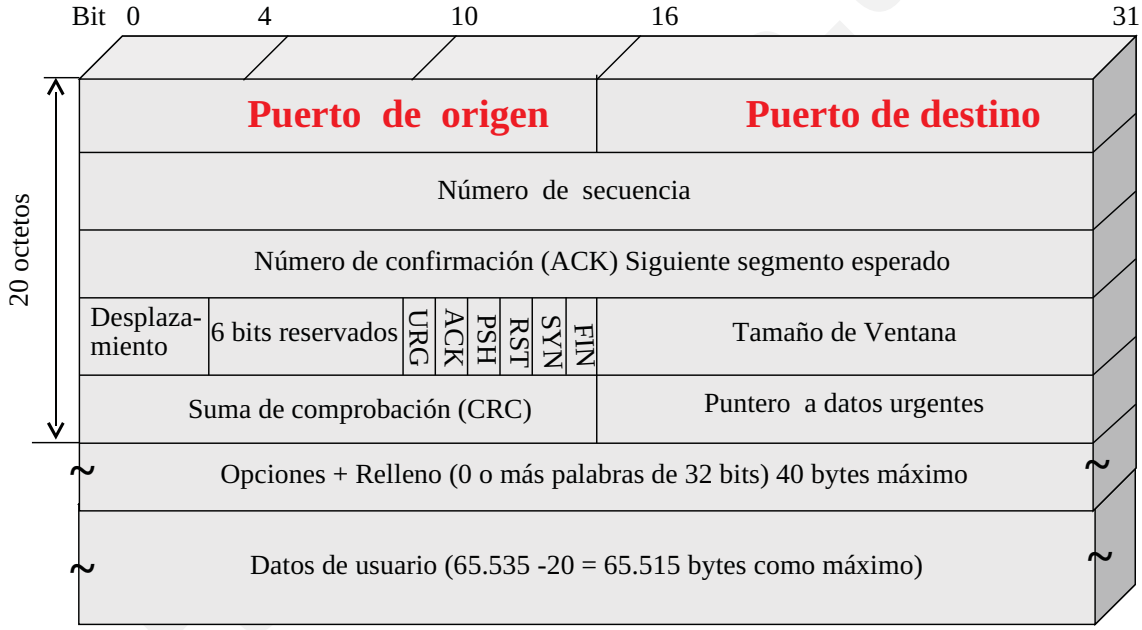
PROTOCOLO BÁSICO: VENTANA DESLIZANTE

- Complicaciones:
  - Fragmentación.
  - Pérdidas de ACK.
  - Duplicaciones de segmentos.
  - Desorden de segmentos.

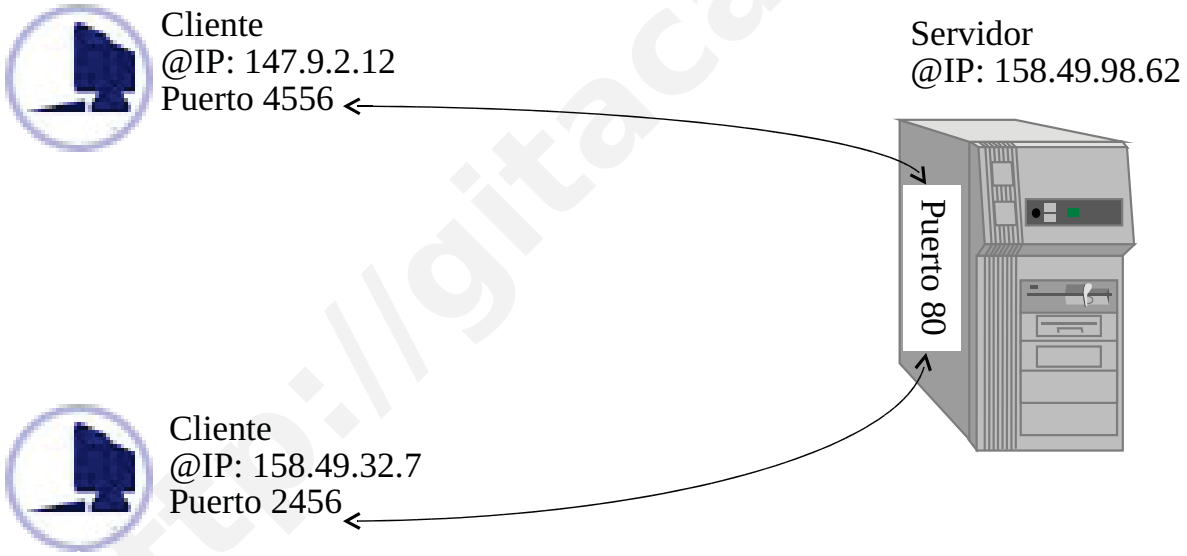
Segmento: Cabecera de formato fijo de 20 octetos, seguida de opciones de cabecera. Tras las opciones (si hay) 65.535 - 20 cabecera = 65.515 octetos de datos.
Se pueden usar segmentos sin datos para ACKs y mensajes de control.



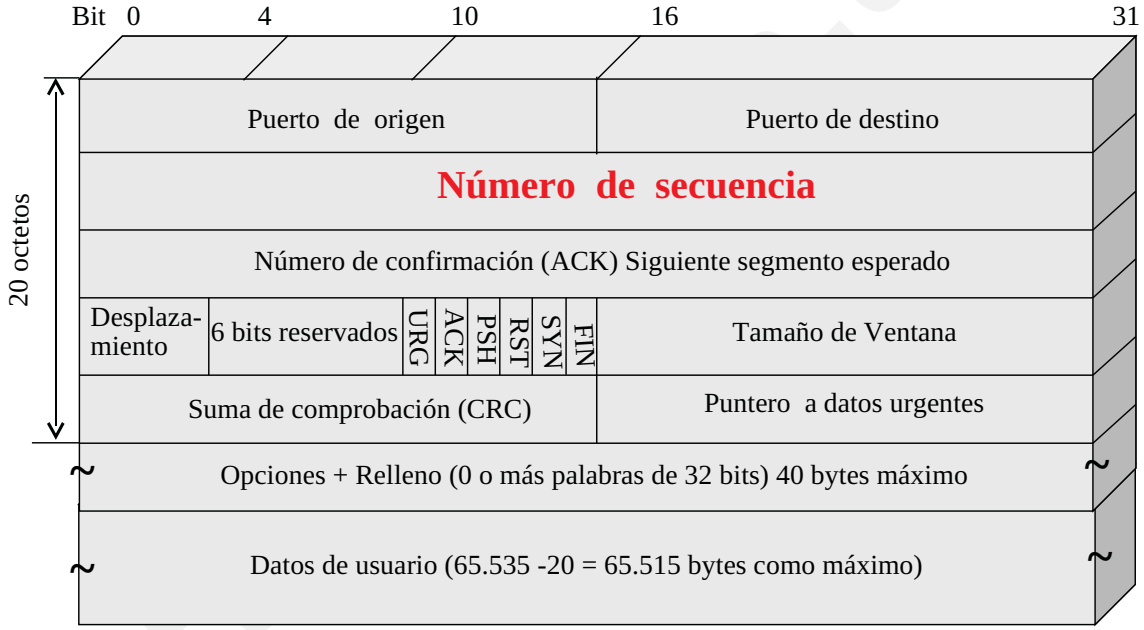
Puertos origen y destino: @IP + NºPuerto (*well-known ports*) (16 bits). Identifican puntos terminales locales de la conexión. Cada host decide la forma de asignar los puertos comenzando por el 256 (16 bits).



Puertos origen y destino: La combinación de una @ IP y el puerto que se usa en la comunicación se denomina *socket*. Una conexión de TCP queda completamente definida mediante las @ de los sockets de ambos extremos. Las cabeceras de los datagramas contienen las @ IP del emisor, y receptor y las cabeceras de los segmentos TCP contienen los Nº de puerto. La @IP de host+Nº puerto forman TSAP de 48 bits.



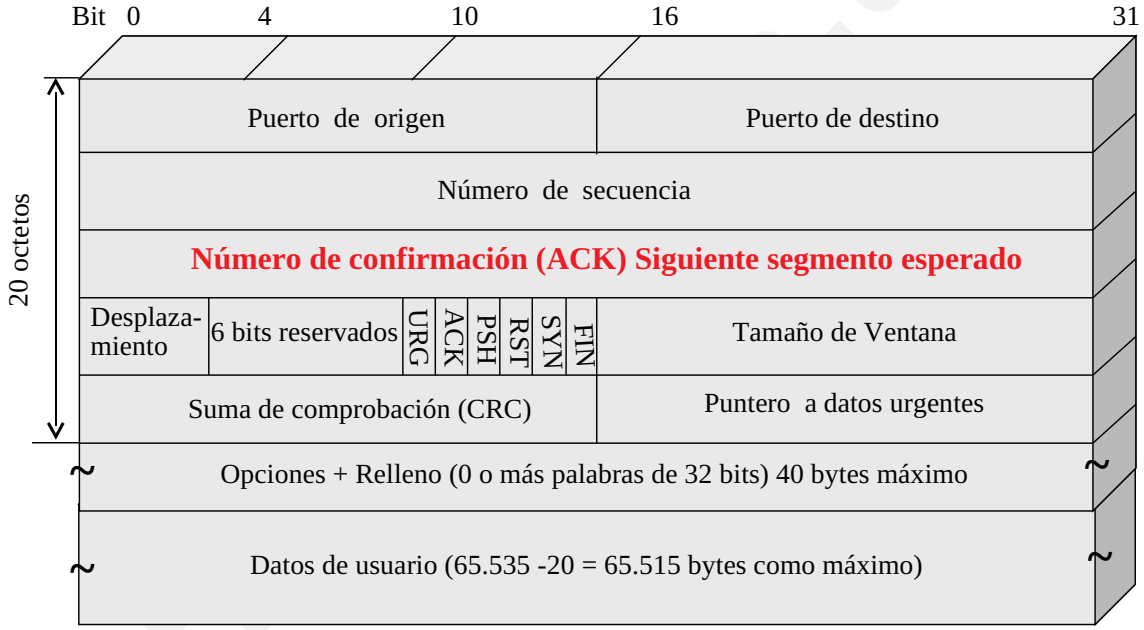
Nº secuencia: Posición, en el caudal de datos, del primer byte (octeto) perteneciente al segmento. (32 bits).



Nº 47

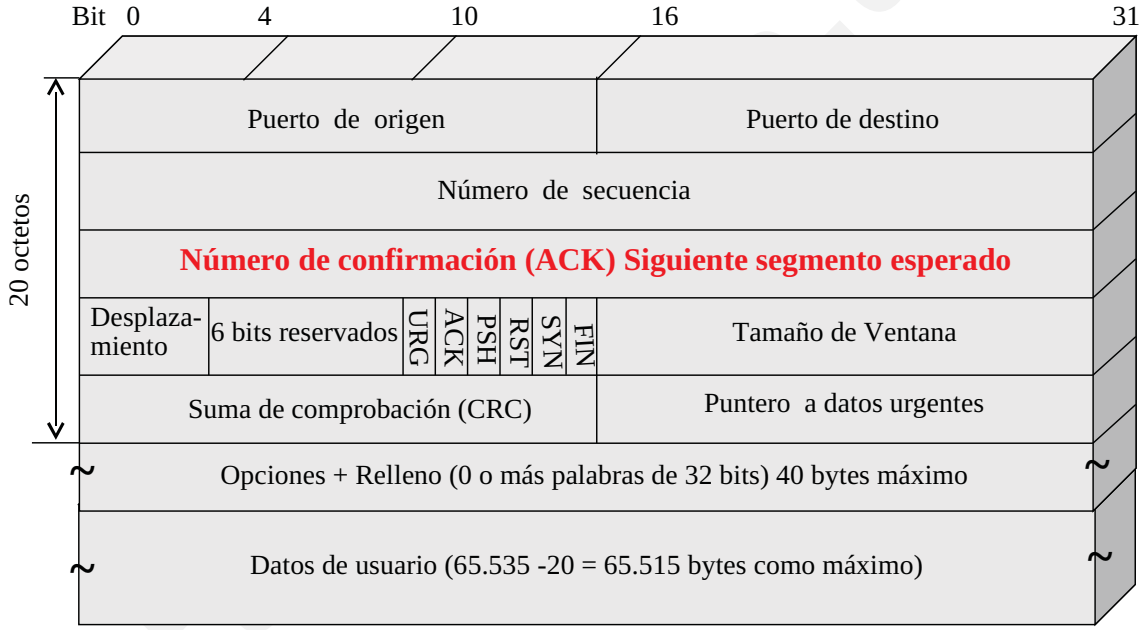
Administración Avanzada de Redes TCP/IP

Nº ACK: Posición, en el *stream*, del byte de menor número que el receptor aún no ha recibido (Nº de secuencia del siguiente byte a recibir). (32 bits). Especifica el siguiente byte esperado, no el último byte correctamente recibido.

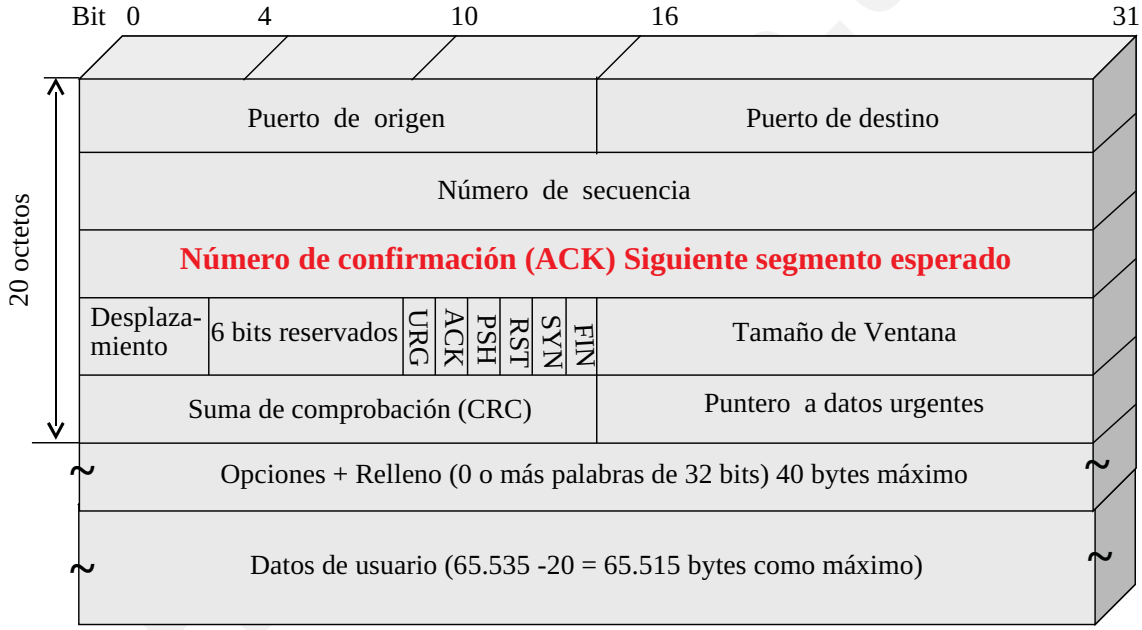


Nº 48

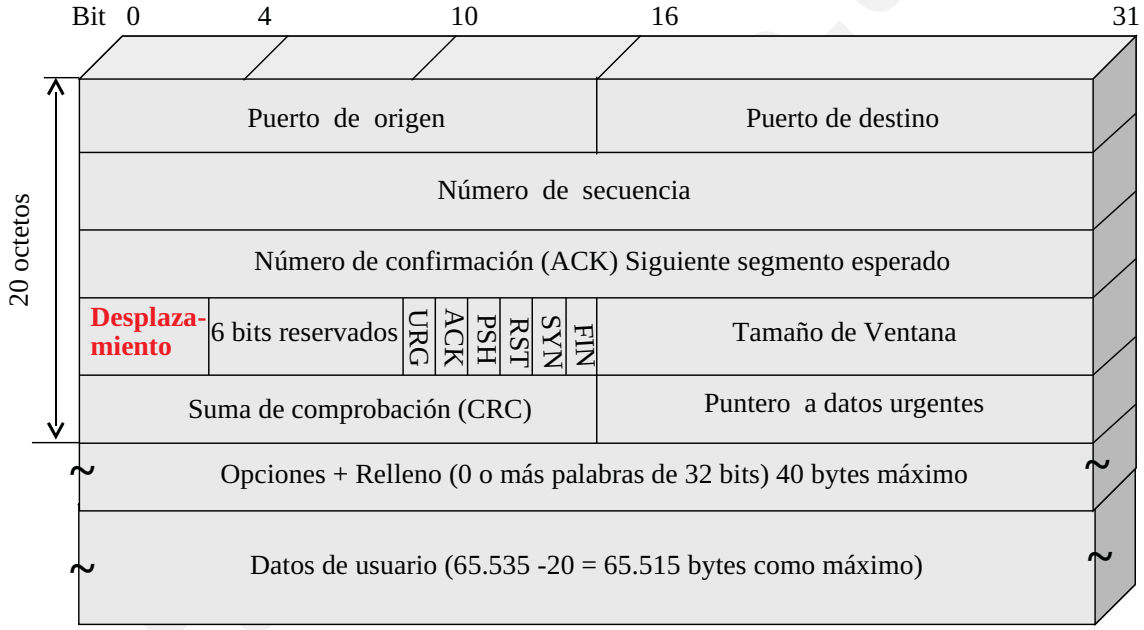
RFC 1106: introduce NAK (*Negative ACK*) para que receptor solicite la retransmisión de un segmento específico y evitar retransmisiones innecesarias debidas a *time-outs*.



RFC 1106: Una vez enviado el segmento a retransmitir el receptor envía los ACK de los datos que tenga en el buffer evitando retransmisiones innecesarias.



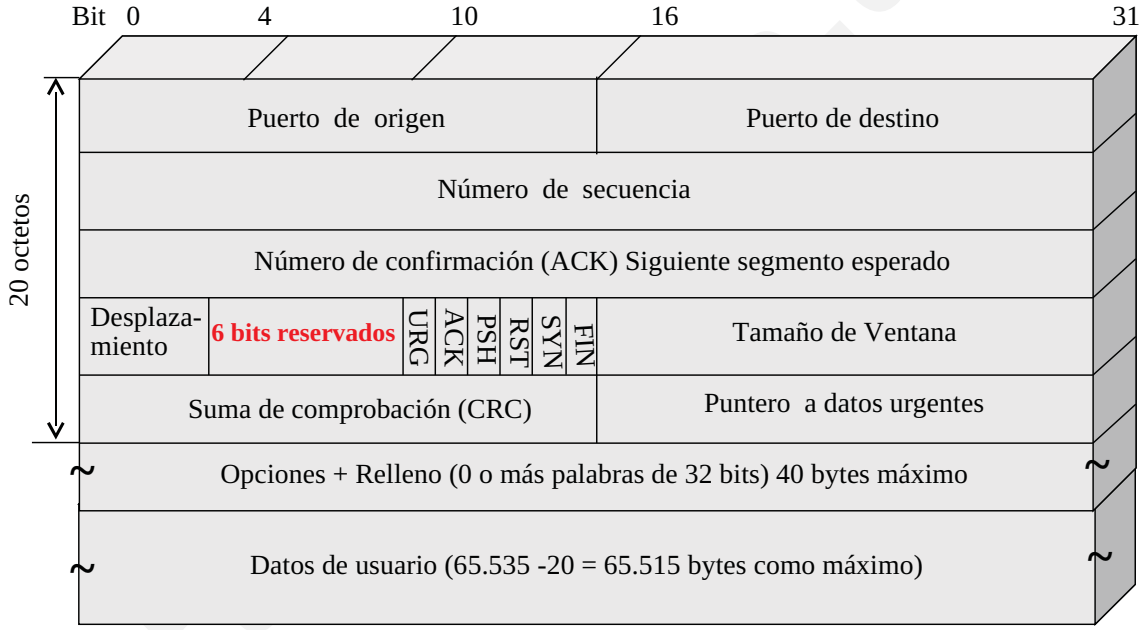
Desplazamiento: O longitud de cabecera (4 bits), indica nº de palabras de 32 bits de la cabecera. Marca comienzo de datos. (4bits). Necesario porque el campo opciones es de longitud variable. Indica comienzo de los datos



Nº 51

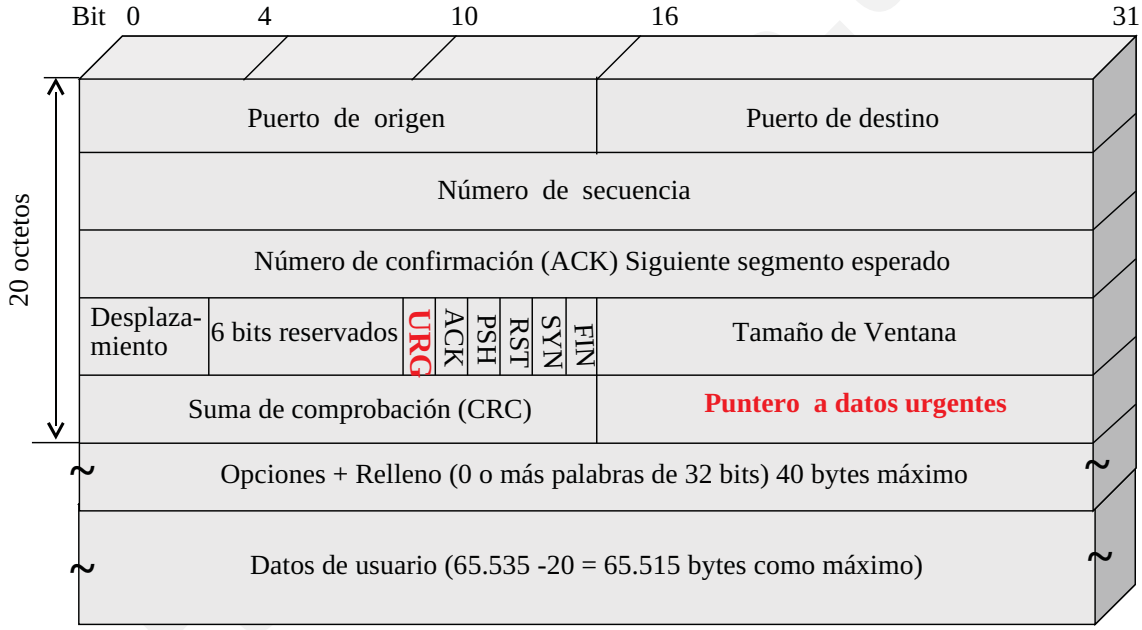
Administración Avanzada de Redes TCP/IP

Reservado: 6 bits no usados pensados para mejorar el protocolo cuando sea necesario. Lleva más de 15 años intacto.



Nº 52

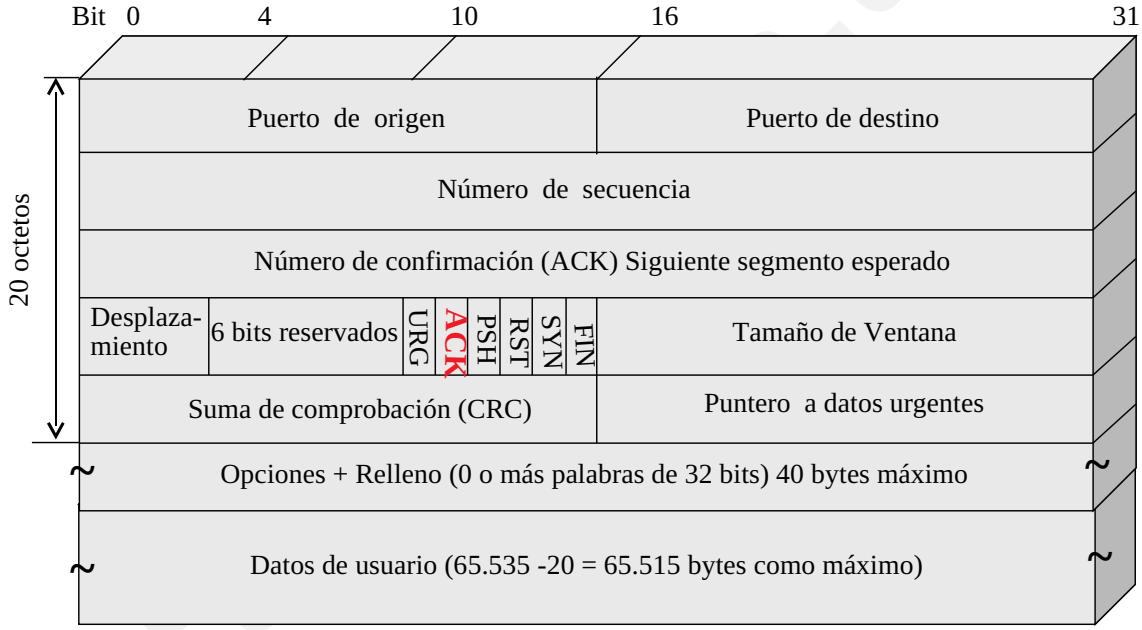
URG: 1 bit que se pone a 1 si se usa el puntero a datos urgente para indicar el comienzo de los datos urgentes.



Nº 53

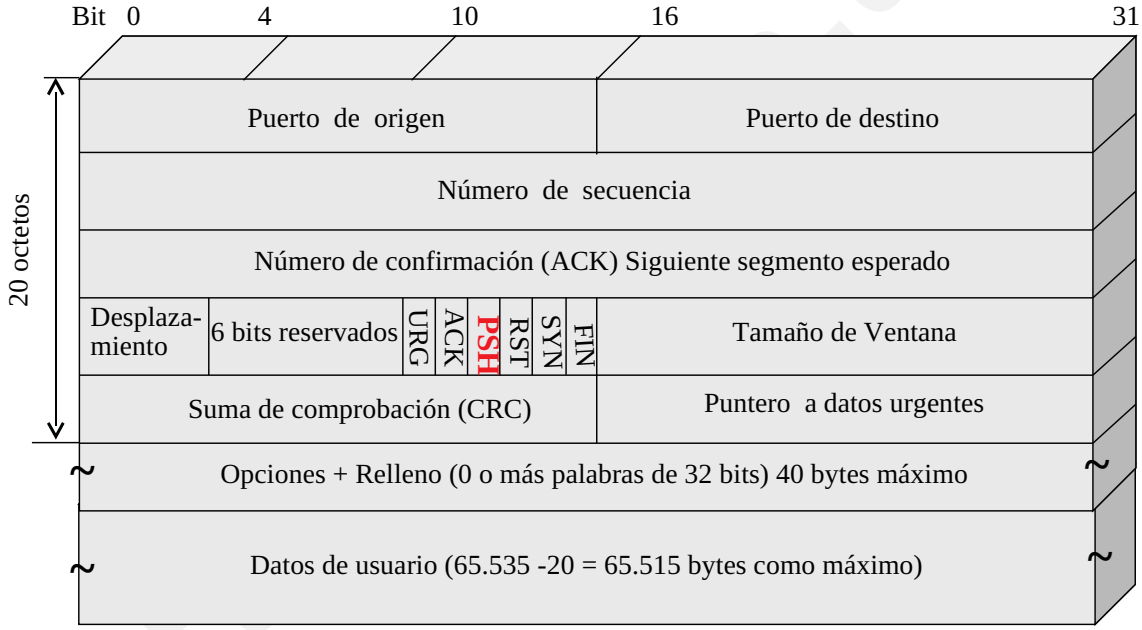
Administración Avanzada de Redes TCP/IP

ACK: Si vale 1 indica que el nº del ACK es válido. Si vale 0 quiere decir que el segmento no contiene un acuse de recibo por lo que se ignora el campo Nº ACK.



Nº 54

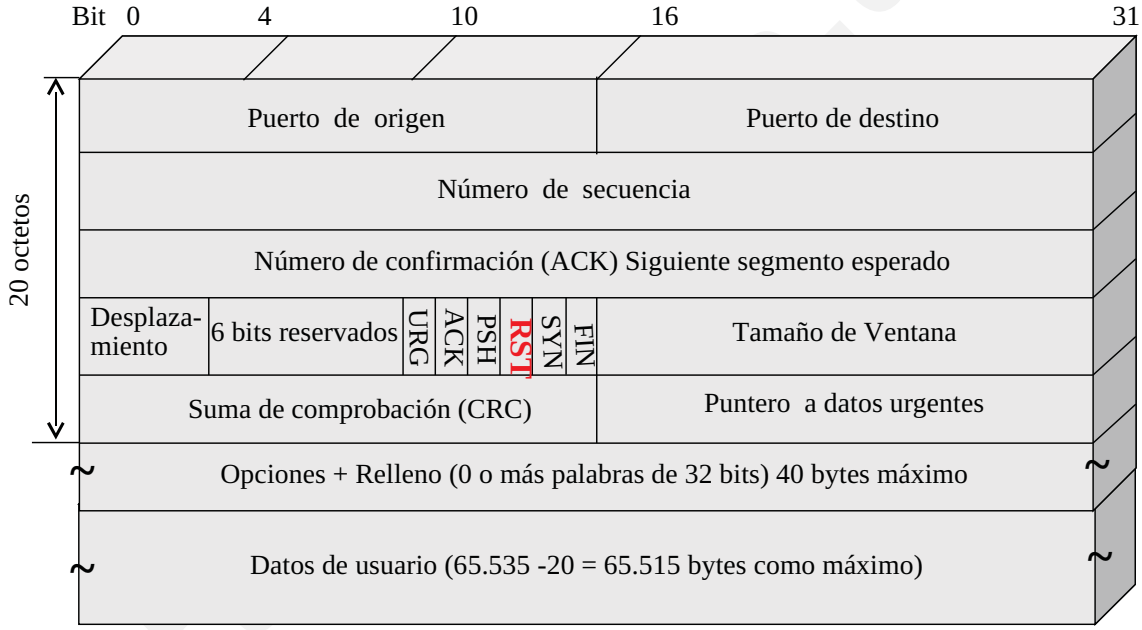
PSH: Datos empujados con *push* para que el receptor no los almacene en el buffer y los pase rápido a la aplicación sin esperar a la situación de buffer completo.



Nº 55

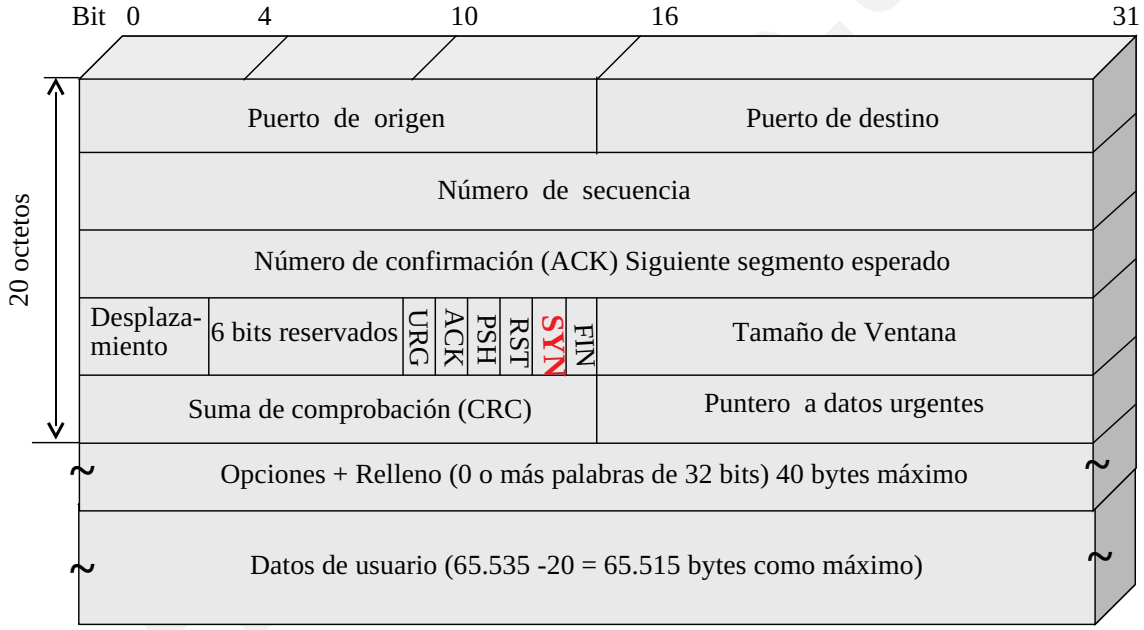
Administración Avanzada de Redes TCP/IP

RST: Se activa a 1 para reestablecer la conexión cuando aparecen problemas (nodo caído, segmentos erróneos, etc.). También sirve para rechazar un segmento no válido o un intento de apertura de conexión.



Nº 56

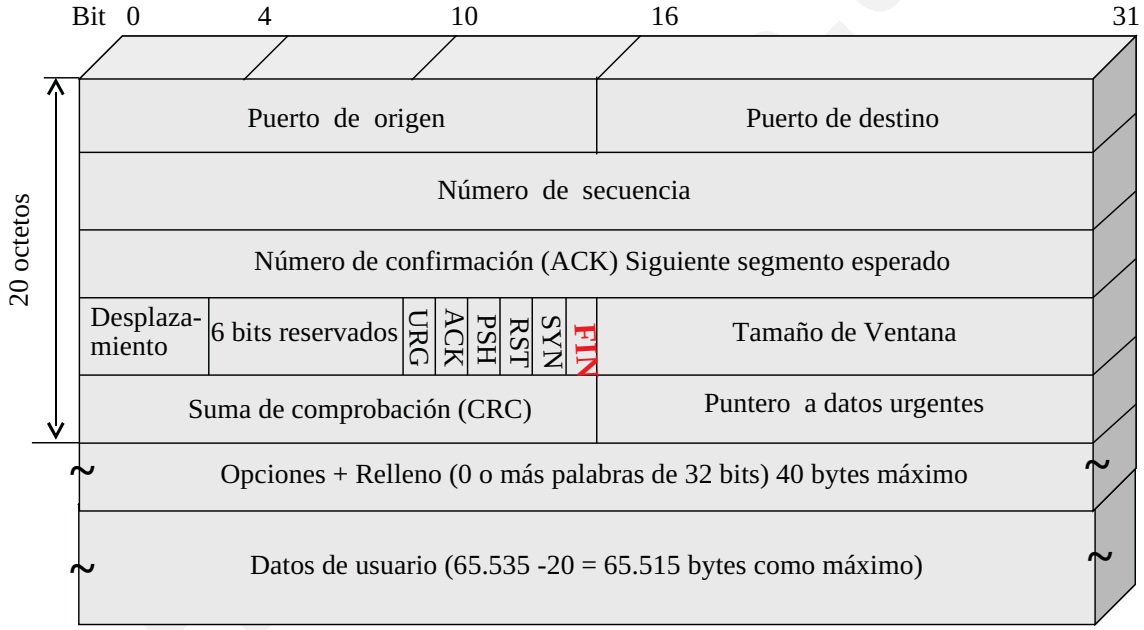
SYN: Para establecer conexiones. (*Connection request* SYN=1 y ACK=0) (*Connection accepted*: SYN=1 y ACK=1).



Nº 57

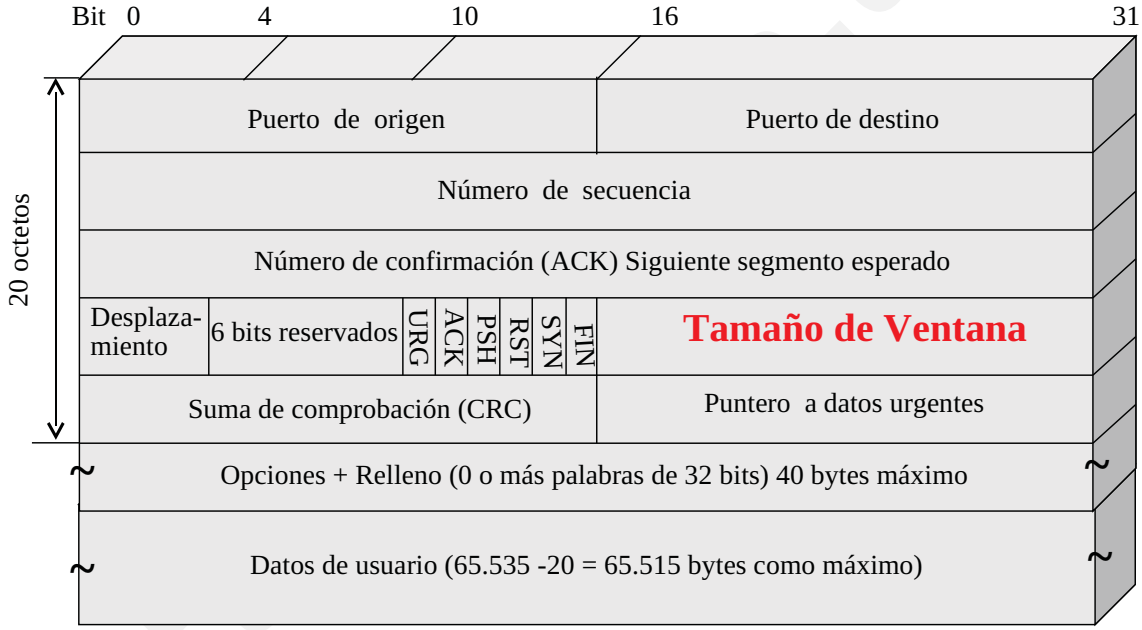
Administración Avanzada de Redes TCP/IP

FIN: Libera la conexión. Especifica que el emisor no tiene más datos para transmitir. No obstante, un proceso puede seguir recibiendo datos indefinidamente. Los segmentos SYN y FIN tienen nº de secuencia y garantía de proceso ordenado.



Nº 58

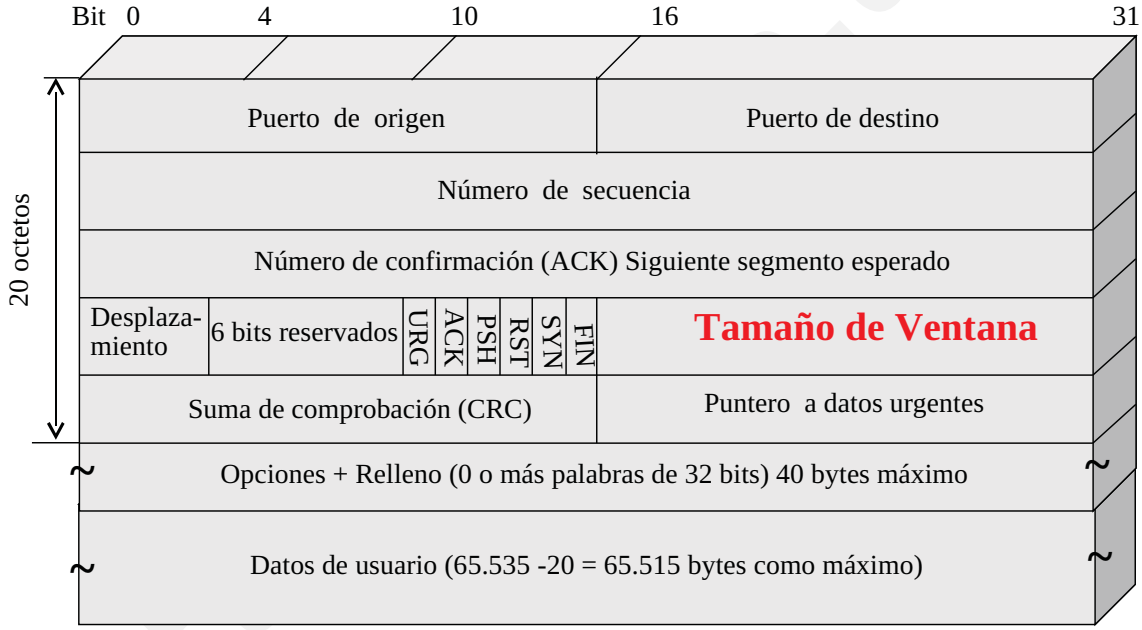
Ventana: Para control de flujo mediante ventana deslizante de tamaño variable. Indica cantidad de bytes que puede enviarse comenzando por el byte del que ya se ha enviado acuse de recibo.



Nº 59

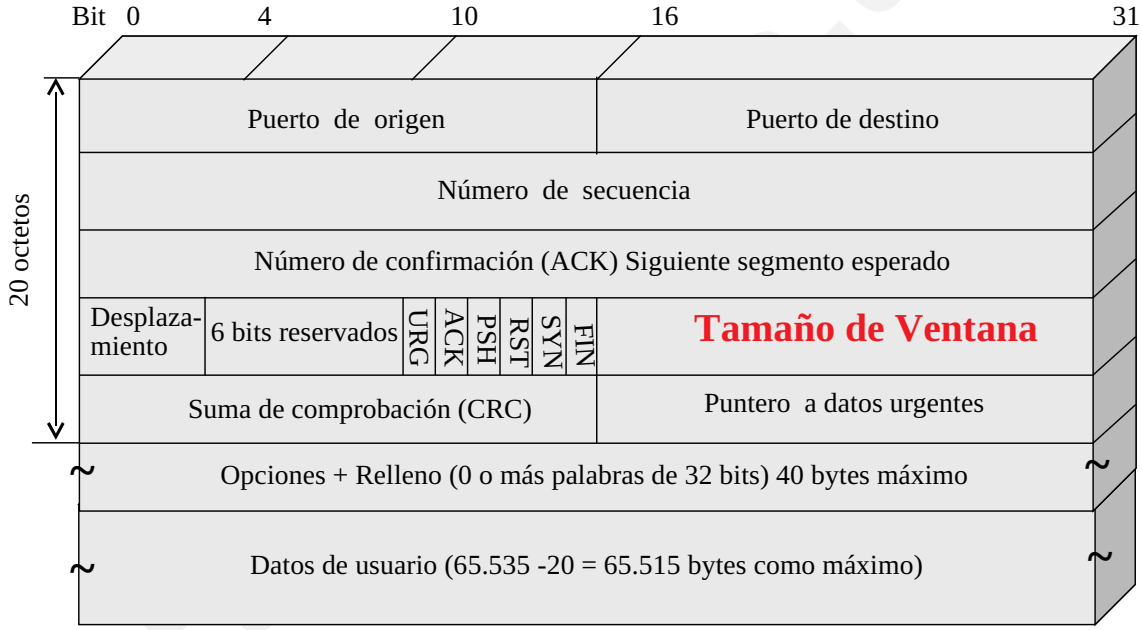
Administración Avanzada de Redes TCP/IP

Ventana = 0 indica que se han recibido todos los bytes hasta Nº ACK-1 pero que el receptor no desea recibir datos de momento. Se puede reiniciar el envío generando el receptor un segmento con el mismo número de ACK y un campo de ventana ≠ de 0.



Nº 60

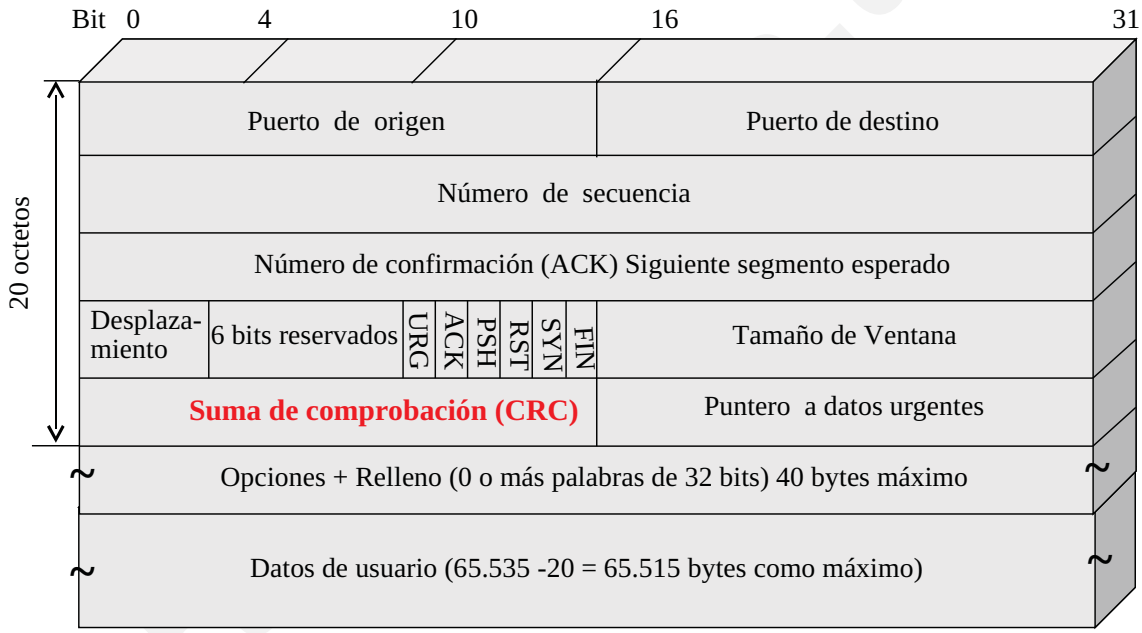
RFC 1323: Escala de ventana para desplazar 16 bits a la izquierda aportando una ventana de hasta 2^{32} bytes soportada en las versiones TCP actuales.



Nº 61

Administración Avanzada de Redes TCP/IP

CRC: Suma de comprobación (CRC) para lograr fiabilidad. Es un CRC de la cabecera, los datos y la siguiente pseudocabecera:



Nº 62

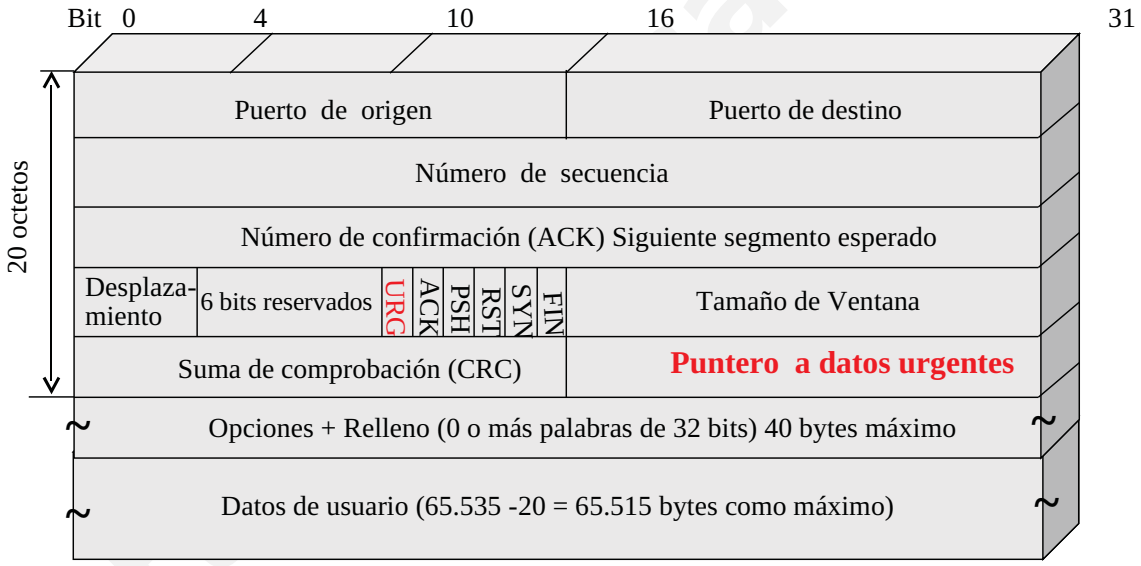
CRC: Suma de comprobación (CRC) para lograr fiabilidad. Es un CRC de la cabecera, los datos y la siguiente pseudocabecera:

32 bits

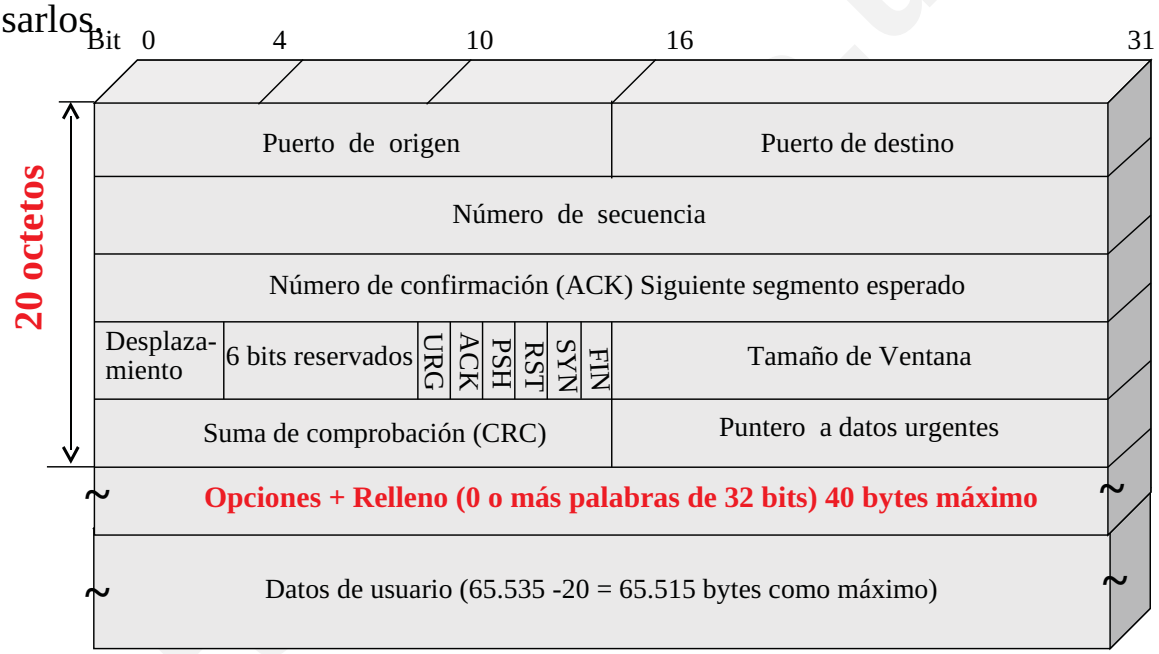
Dirección IP nodo origen		
Dirección IP nodo destino		
00000000	Nº protocolo TCP=6	Longitud de segmento TCP

- Algoritmo CRC suma todas las palabras de 16 bits complemento a 1 y luego obtiene el complemento a 1 de la suma. Como consecuencia, al hacer el receptor el cálculo con el segmento completo (incluido CRC) el resultado debe ser 0.
- Incluir las @ IP permite detectar paquetes mal entregados pero viola la jerarquía de protocolos ya que pertenecen a la capa IP y no a la TCP.

Puntero a datos urgentes: Válido si está activo el bit URG. Es un puntero que indica un desplazamiento en bytes a partir del número actual de secuencia en el que se encuentran datos urgentes. Mecanismo rudimentario para sustituir a los mensajes de interrupción que permite que el emisor envíe una señal al receptor sin implicar a TCP en la razón de la interrupción.



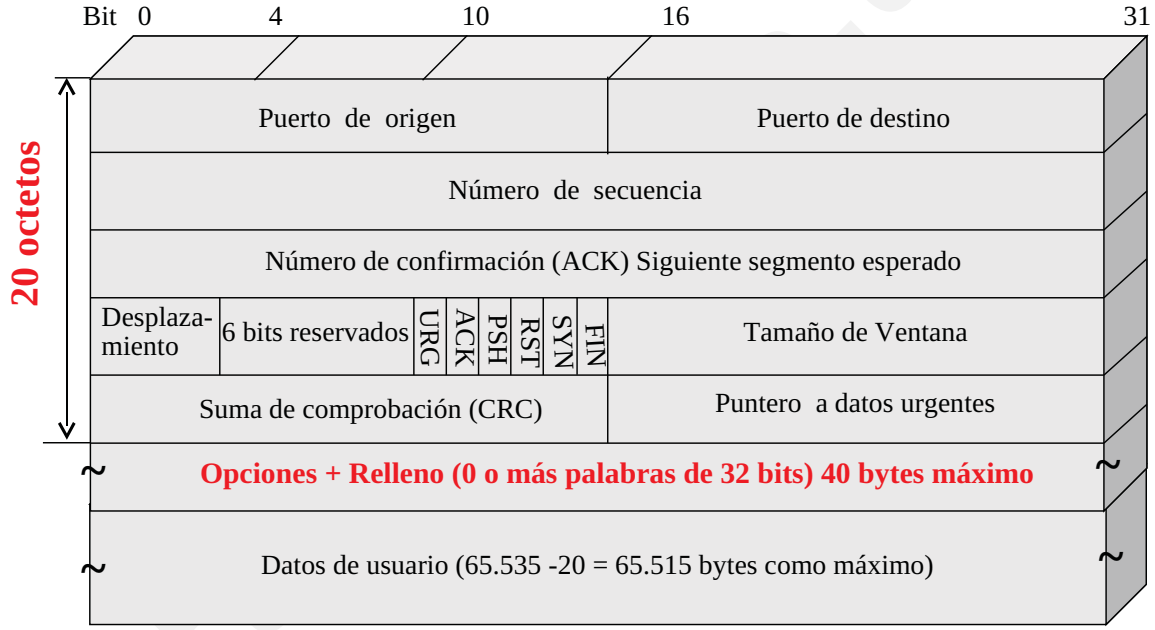
Campo opciones: Para poder añadir características no cubiertas por la cabecera fija. Por ejemplo: nodos especifiquen la carga útil máxima que pueden aceptar. Usar segmentos grandes es más eficiente, pero hay nodos que no pueden procesarlos.



Nº 65

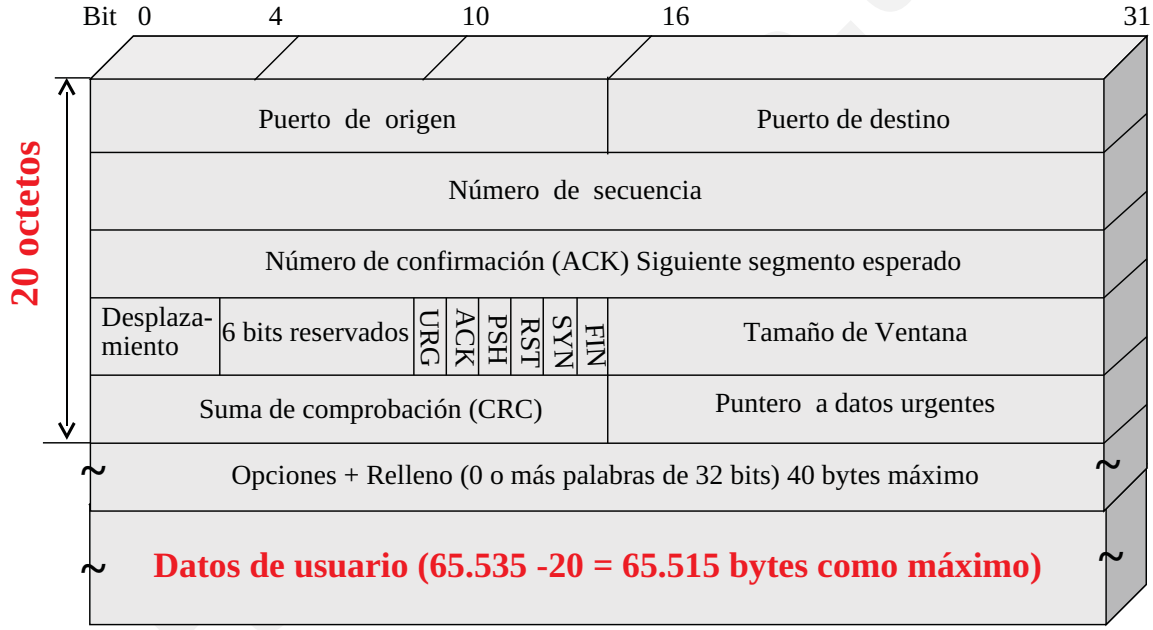
Administración Avanzada de Redes TCP/IP

Campo opciones: En el establecimiento cada nodo anuncia su máximo y puede conocer el del otro extremo. Se elige el más pequeño de ambos. Si no se define valor alguno el tamaño por defecto de los segmentos es de 536+20= 556 octetos.

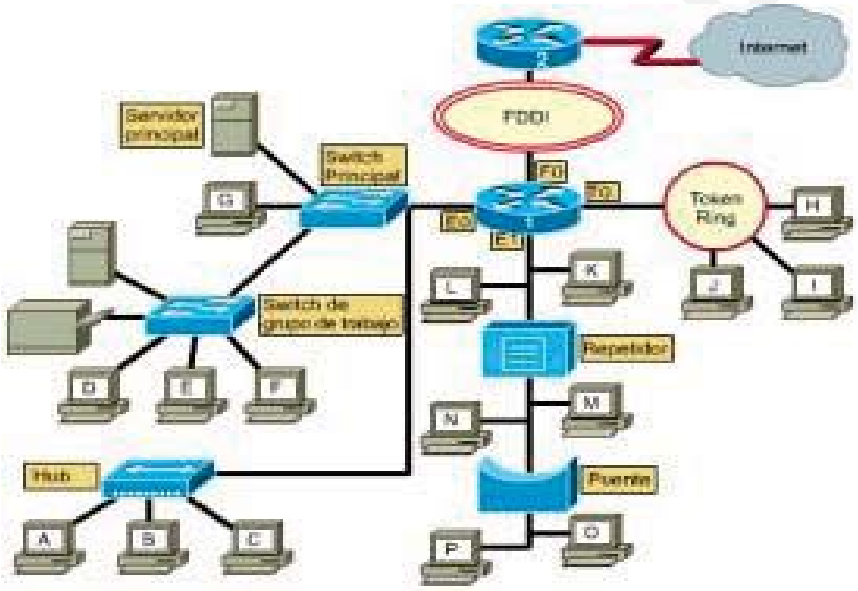


Nº 66

Datos de usuario: Datos usuario realmente transmitidos que se encapsulan con los 20 octetos de la cabecera TCP y los opcionales 40 octetos del campo Opciones.



2. Conceptos básicos: encaminamiento, direccionamiento, etc.



Direccionamiento IP

• En una red IP, cada PC tiene asignada una dirección IP que le identifica de manera única en la red. Está formada por un identificador de red y un identificador de nodo.

• En el caso de routers o gateways, cada interfaz de red tiene un identificador de red diferente.

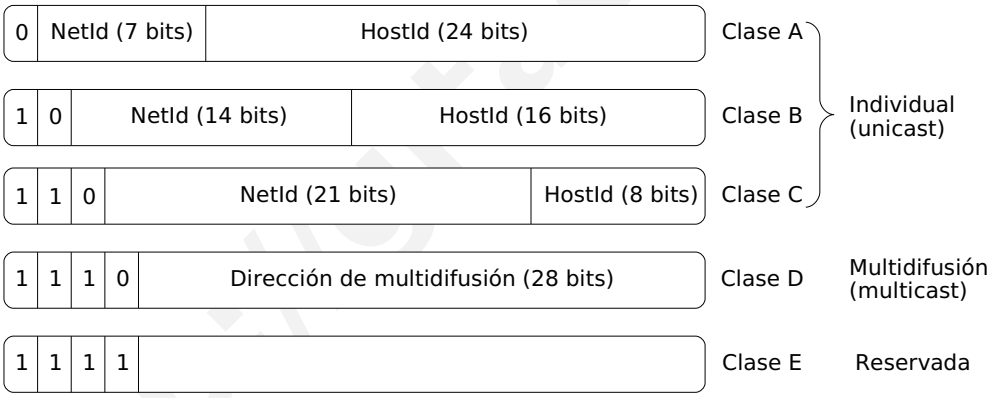
• Se han utilizado hasta 5 esquemas de asignación de direcciones IP en la historia de Internet:

- Basadas en clases: divide el espacio de dir. en las clases A, B, C, D y E.
- Subredes: se emplea la máscara de subred para limitar subred/hostid.
- Sin clase: permite uso más eficiente del espacio de direcciones.
- NAT: cada red tiene IP única y todos los PCs la comparten hacia fuera.
- Ipv6: desarrollada para resolver el problema de la limitación de dirs.

Direcciones basadas en clases

• Consistía en dividir el espacio de direcciones de 32 bits en 5 clases, cada una pensada para redes de distinto tamaño.

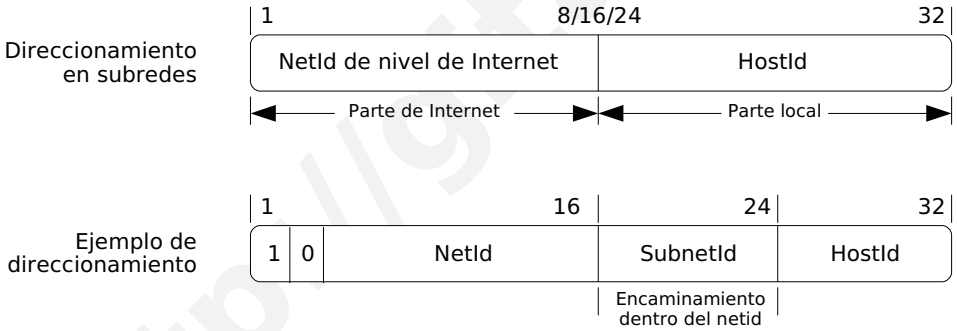
• La clase a la que pertenece una dirección se determina por la posición que ocupe el primer 0 entre los 4 bits de mayor peso.



Subredes

• El concepto de subnetting fue introducido para separar las funciones de encaminamiento de una organización particular de las de la interred global.

• En lugar de que cada LAN de la organización tenga su propio *netid*, se usa solo un *netid* para toda la organización. Cada LAN será una subred y formará parte del campo *hostid*.



Direccionamiento sin clases

• En este esuqema, la parte que identifica a la red dentro de la dirección IP puede comprender cualquier número de bits, en lugar de estar restringido a los límites de las clases fijas.

• Tiene la forma *x.x.x.x/n*, donde *n* indica el número de bits que ocupa la parte *netid* dentro de la dirección.

• Si una organización necesita direccionar 1000 PCs (1024 dirs.), la representación en notación de punto sería x.x.x.x/22.

• Se puede seguir empleando la técnica de división en subredes para la parte *hostid*.

• Es un esquema que permite un uso muy eficiente del espacio de direcciones, pero el encaminamiento de paquetes es más complejo

Encaminamiento estático

• El encaminamiento es el mecanismo empleado en una red de interconexión para determinar la ruta óptima hacia un destino.

• Consiste en que la información que debe usarse para alcanzar el nodo destino se almacena en las tablas de encaminamiento de los nodos cuando éstos se ponen en funcionamiento.

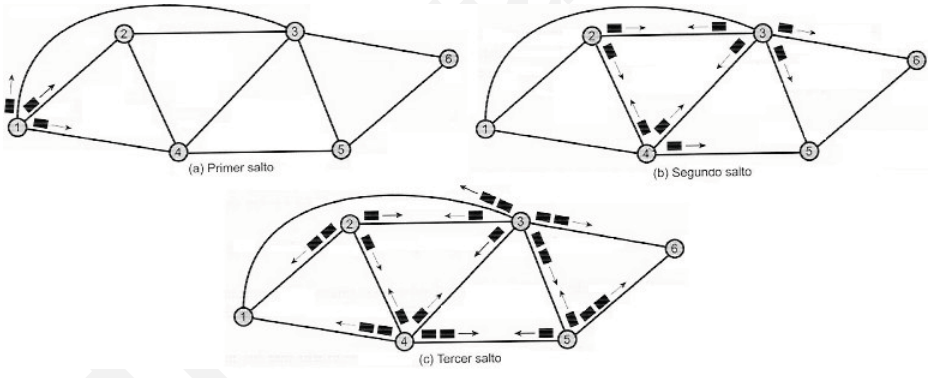
• En caso de existir múltiples caminos hacia el destino se suele utilizar una segunda métrica, como por ejemplo la distancia.

• Desventaja: los cambios en la topología o los fallos implican modificar las tablas de encaminamiento de todos los routers. Por tanto es inapropiado para redes grandes o con cambios frecuentes, como Internet.

Inundación (flooding)

• En el encaminamiento por inundación, cuando un nodo recibe un paquete, reenvía una copia a cada uno de los nodos con los que está conectado

• La info. suele alcanza el destino a través de la ruta óptima, pero a costa de una fuerte sobrecarga. Usado sólo en fases de inicialización, para que los routers conozcan la topología.



Vectores de distancia

• Algoritmo distribuido empleado por routers para construir su tabla de encaminamiento (el vector) que contiene el coste de cada camino (la distancia) para alcanzar cualquier destino.

• Inicialmente cada router sólo conoce sólo los nodos a los que está directamente conectado (tabla de adyacencia).

• Para construir las tablas completas, cada router envía (en intervalos predefinidos) su tabla actualizada con los vecinos y las distancias que él conoce.

• Es más eficiente que flooding poruqe sólo se emplea una ruta para intentar llegar al destino, pero las actualizaciones implican overhead y coste de procesamiento en nodos. Además los paquetes pueden entrar en bucles en lugar de ir directamente al destino.

Estado de enlaces y camino más corto

• Inicialmente cada router sólo conoce su propia tabla de conectividad o adyacencia.

• Periodicamente cada nodo difunde a sus vecinos inmediatos un mensaje de estado de los enlaces, con cada router que conoce y su info de conectividad asociada. Si no existiera conectividad entre dos nodos, la distancia entre ambos se considera infinita.

• Objetivo: elegir el camino más corto (Dijkstra) desde cualquier nodo de la topología hacia el resto.

• Si existe empate entre varias rutas, se elige una arbitrariamente, pero se conservan todas en la tabla; de esta forma se hará posible compartir la carga entre todas: Ingeniería de Tráfico.

•Aparte de la distancia se pueden asociar otros costes o restricciones a los enlaces (ancho de banda disponible, retardo, ...)

Encapsulado en túnel

• Internet está formada por muchas redes administradas de forma independiente empleando incluso diferentes protocolos o modos de operación.

• A atravesar redes que operan de distinta forma el enrutado no se hace directamente sino que los flujos se encapsulan siguiendo la técnica de *tunneling*.

• Se necesitan nodos encaminadores especiales multiprotocolo, que tomaran los paquetes del primer protocolo para encapsularlos en paquetes del segundo, para que se puedan encaminar según las reglas de la segunda red.

• A la salida se sigue el proceso inverso, la pasarela de salida desencapsulará los paquetes, haciendo que el paso por la red "diferente" se haga transparente.

Encaminamiento por difusión

• Es un encaminamiento orientado a redes de área local (LANs), en el que se tendrá en cuenta las direcciones físicas (MAC).

• Cada nodo del segmento LAN aceptará una trama particular si la dirección MAC de destino coincide con la suya, si es la de difusión o si es una dirección de grupo y pertenece a dicho grupo.

- Difusión limitada: se envía la info a todos los nodos del segmento LAN. Se emplea 255.255.255.255 como IP destino.
- Difusión hacia una subred: se emplea la máscara de red de la subred destino.
- Difusión hacia una red: se envía copias a todos los PCs conectados a la red especificada en la IP de destino. El problema aquí es cómo difundir los paquetes a todas las subredes que forman parte de la red destino.

Pruebas de direccionamiento

- *Traceroute* es un comando que permite obtener los equipos por los que pasan los paquetes IP hasta llegar a su destino. Permite también analizar el estado de carga de una red.
- Emplea dos caracerísticas de TCP/IP:
  - *TTL*: número de saltos límite de un datagrama antes de ser desechado por la red.
  - *ICMP*: sirve para manejar mensajes de control y error.
- Con ambas características *traceroute* permite obtener un mapa de la red de acuerdo a cómo la ve un nodo particular.
- Para cada *hop* se enviarán 3 paquetes con un *TTL* que se va incrementando paulatinamente. Se mostrará el nodo que responde junto con las métricas de tiempo empleado.

Administración Avanzada de Redes TCP/IP

Traceroute: prueba 1

```
# traceroute www.unex.es

traceroute to sntrv-proxy.unex.es (158.49.17.45), 30 hops max, 38 byte packets
1  158.49.98.126 (158.49.98.126)  5.819 ms  0.234 ms  0.195 ms
2  158.49.129.3 (158.49.129.3)  1.307 ms  1.314 ms  1.165 ms
3  158.49.254.1 (158.49.254.1)  5.406 ms  4.863 ms  14.152 ms
4  * * *
5  * * *
...
29  * * *
30  * * *
```

Los asteriscos ' * ' pueden indicar que el host correspondiente al *hop* puede tener algún tipo de protección contra este tipo de comandos.

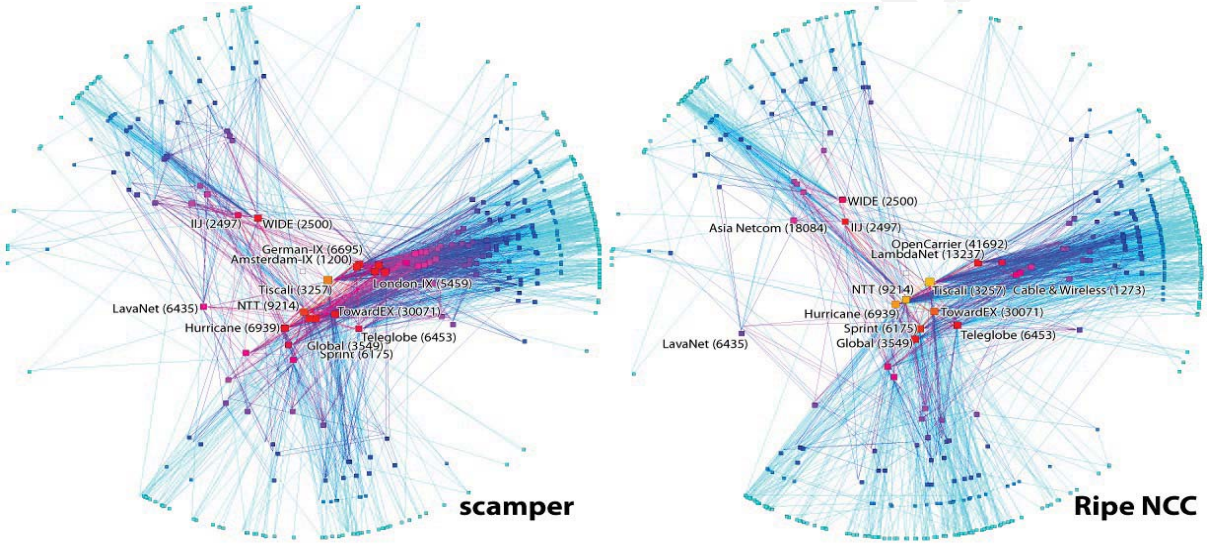
Traceroute: prueba 2

```
#  traceroute ftp.rediris.es

traceroute to zeppo.rediris.es (130.206.1.5), 30 hops max, 38 byte packets
1  158.49.98.126 (158.49.98.126)  0.405 ms  0.255 ms  0.212 ms
2  158.49.129.3 (158.49.129.3)  1.263 ms  1.624 ms  1.710 ms
3  158.49.254.1 (158.49.254.1)  5.025 ms  5.586 ms  5.485 ms
4  AT0-0-0-0.EB-Badajoz0.red.rediris.es (130.206.203.5)  5.097 ms  5.048 ms  5.435
ms
5  EXT.SO3-0-0.EB-IRIS4.red.rediris.es (130.206.250.57)  15.702 ms  16.623 ms
13.078 ms
6  CAT6509-2.red.rediris.es (130.206.220.58)  12.811 ms  130.206.220.59
(130.206.220.59)  14.716 ms  13.018 ms
7  zeppo.rediris.es (130.206.1.5)  14.236 ms  14.536 ms  12.527 ms
```

Traceroute: prueba 3

```
# traceroute www.google.es
traceroute: Warning: www.google.es has multiple addresses; using 209.85.129.99
traceroute to www.l.google.com (209.85.129.99), 30 hops max, 38 byte packets
1  158.49.98.126 (158.49.98.126)  0.350 ms  0.261 ms  0.245 ms
2  158.49.129.3 (158.49.129.3)  1.167 ms  1.010 ms  0.969 ms
3  158.49.254.1 (158.49.254.1)  5.168 ms  4.789 ms  5.242 ms
4  AT0-0-0-0.EB-Badajoz0.red.rediris.es (130.206.203.5) 6.220 ms 5.646 ms 5.887 ms
5  EXT.SO3-0-0.EB-IRIS4.red.rediris.es (130.206.250.57)  12.650 ms  13.753 ms  13.146 ms
6  mad-b1-link.telia.net (213.248.70.249)  14.592 ms  14.216 ms  12.303 ms
7  prs-bb2-pos1-2-0.telia.net (213.248.64.129)  40.282 ms  41.831 ms  40.807 ms
8  ffm-bb2-link.telia.net (80.91.249.46)  50.067 ms  49.147 ms  49.933 ms
9  ffm-b6-link.telia.net (80.91.251.161)  68.920 ms  49.849 ms  49.950 ms
10  google-ic-120086-ffm-b6.c.telia.net (80.239.193.138)  49.804 ms  49.970 ms  49.177 ms
11  72.14.232.205 (72.14.232.205)  49.764 ms  50.621 ms  49.652 ms
12  72.14.233.206 (72.14.233.206)  62.389 ms  56.075 ms  53.638 ms
13  fk-in-f99.google.com (209.85.129.99)  50.795 ms  51.207 ms  50.628 ms
```

BGP - *Border Gateway Protocol*



© Caida.org

Encaminamiento estático

- Llegar a destinos no locales: direcciones IP, clases de red, máscaras de red, tabla de encaminamiento, etc.
- ¿Configuración de los parámetros de red?
  - En hosts.
  - En equipación de red.
- Si la configuración es manual debe estar basada en documentación de red.

Encaminamiento estático: ventajas e inconvenientes

- Ventajas:
  - No es necesario despliegue de protocolos de encaminamiento: Despliegue más sencillo en redes pequeñas.
  - ¿?
- Inconvenientes.
  - Inadecuado para organizaciones con un diseño de red complejo.
  - Inadecuado para redes con cambios topológicos.
  - Inadecuado para redes tolerantes a fallos o que transporten tráfico difícilmente predecible.
  - ¿?

Encaminamiento adaptativo

- Dos familias:
  - *Interior Gateway Protocol* (*IGP*)
  - *Exterior Gateway Protocol* (*EGP*)
- Concepto de Sistema Autónomo (*Autonomous System* o *AS*):
  - Conjunto de redes IP y routers bajo una misma autoridad administrativa que presenta una misma política de encaminamiento hacia Internet.
- IGP definido por la autoridad administrativa del AS. Encaminamiento Intra-AS.
- EGP común para conseguir encaminamiento Inter-AS.

Encaminamiento adaptativo. RIP

- RIP (*Routing Information Protocol*) es un protocolo IGP simple basado en vector-distancia.
- El primer desarrollo de RIP fue un componente del código de red de Berkeley UNIX, llamado routed (*route management daemon*).
- RIPv1 (RFC1058, 1988) se desarrolló para requerir una cantidad de configuración mínima y de una complejidad de desarrollo pequeña (debido a la simplicidad del protocolo) para facilitar su despliegue.
- RIPv2 (RFC 2453, 1993-1998) mantiene objetivos de RIPv1, pero soporta CIDR, autenticación de actualizaciones y sustitución de *broadcasting* por *multicasting*.

RIPv1: Características

- Las direcciones presentes en las tablas RIP son direcciones IP de 32 bits.
- Una entrada en las tablas de routing puede representar:
  - Un host
  - Una red
  - Una subred
- Inicialmente se separa la parte de dirección de red de la parte “subred + host”, como una función dependiente de la clase de red.
- Si “subred + host” es nulo, la dirección representa a una red.
- Si no es nulo, la dirección representa a una subred o un host.

RIPv1: Características

- Utiliza el hop-count como métrica, con un número máximo de 15 saltos.
- Mecanismos implementados en RIP para evitar que se propague información de routing incorrecta:
  - Holddown (se establece a 180 seg.)
  - Split horizon.
- Las actualizaciones de tablas de encaminamiento (completas) se envían, por defecto, cada 30 seg, mediante broadcasting.
  - ¿Supone esto un problema?
  - ¿Soluciones?

RIPv2

- RIPv2 surge para incorporar las siguientes características:
  - Soporte de CIDR.
  - Incorporación de autenticación (inicialmente basada en texto plano, aunque después se incorpora MD5).
  - Envío de actualizaciones a RIP2-ROUTERS.MCAST.NET (224.0.0.9)

¿Cuándo usar RIP?

- RIP es un protocolo simple, sencillo de desplegar y con una configuración mínima.
- Pero:
  - RIP es inadecuado para redes grandes y complejas.
  - Puede calcular nuevas rutas en caso de cambios topológicos, pero en algunos casos lo hace muy lentamente.
  - Mientras tanto, la red queda en un estado transitorio.
  - Podrían ocurrir ciclos en la red y causarse congestión.
  - Además, está limitado a 15 *hops*.

Encaminamiento adaptativo. OSPF

- Se desarrolla la tecnología de estado de enlace con objeto de solucionar algunos de los problemas de vector-distancia.
- OSPF sucesor natural de RIP, y actual recomendación del IAB.
- En lugar de intercambiar distancias a cada destino, se mantiene un "mapa" de la red que se actualiza rápidamente tras cada cambio en la topología.
- Se podría utilizar cualquier algoritmo para el cálculo de rutas, dada una base de datos de estado de enlace.
- OSPF (*Open Shortest Path First*) utiliza el algoritmo SPF.
- OSPFv1 (RFC 1131, 1989), OSPFv2 (RFC 1583, 1994), OSPFv3 (RFC 2740, 1999)

OSPF: ¿Por qué es mejor?

- Convergencia más rápida y sin crear ciclos.
- Soporte de métricas múltiples. (¿Cuáles?, ¿Para qué?)
- Soporte de varias rutas a un mismo destino. (¿Para qué?)
- Representación independiente para las rutas externas.

Características de OSPF

- Métrica basada en el *path cost*.
- Jerárquico: posibilidad de dividir un AS (*Autonomous System*) en varias áreas.
- No utiliza ni TCP ni UDP, sino IP directamente.
- Subprotocolos:
  - *Hello Protocol*
  - *Exchange Protocol*
  - *Flooding Protocol*

Encaminamiento adaptativo. IS-IS

- RIP y OSPF: propuestas IGP del IETF.
- OSI tiene la suya: IS-IS (*Intra-Domain Intermediate System to Intermediate System Routing Protocol*)
- Al igual que OSPF, es un protocolo de estado de enlace.
- Comparado con OSPF:
  - IS-IS no encamina de forma nativa paquetes IP.
  - Los subprotocolos son distintos, si bien los conceptos son similares.
  - Aunque OSPF ha sido extendido por su popularidad, IS-IS generalmente escala mejor en grandes redes.
  - OSPF soporta < 50 routers en un área. IS-IS < 1000
  - IS-IS es más neutral con respecto a las direcciones de red.

BGP – Hasta ahora...

- El tráfico circulante por una red usa para guiarse protocolos de encaminamiento interior como IS-IS u OSPF.
- Los protocolos de encaminamiento interior no saben cómo guiar el tráfico más allá del límite de la red sobre la que actúan.

¡no podemos hacer llegar tráfico desde España a China!

BGP - Problemática gral. del encamin. Interdominio (I)

- Una de las palabras claves dentro del encaminamiento interdominio es la de **Sistema Autónomo** (AS).
- Un AS se puede entender como un conjunto de nodos administrados por una misma **entidad organizativa** y que siguen una misma política de encaminamiento.
- Una entidad organizativa puede ser una empresa, un proveedor de servicios, una organización gubernamental, una entidad académica, etcétera.
- En cada AS, la entidad organizativa es propietaria de la red, organiza los recursos a su antojo, aplica las políticas de encaminamiento que desea según los fines que le mueven, realiza cambios en la topología, conduce el tráfico, aplica técnicas de ingeniería de tráfico... ¡Cada uno manda en su casa!
- Mientras en encaminamiento interior la entidad organizativa tiene el control completo de una comunicación desde el origen al destino, no ocurre igual en el encaminamiento interdominio, donde las comunicaciones “salen fuera”.

BGP - Problemática gral. del encamin. Interdominio (II)

- Los AS se necesitan los unos a los otros puesto que una comunicación puede extenderse sobre varios de ellos.
- Sin embargo, a nadie le gusta que le digan cómo debe gestionar su propia red y nadie desea que los demás sepan cómo se hacen las cosas dentro de su sistema autónomo. ¡los trapos sucios quedan en casa!
- Ejemplos:
  - ¿Qué pasaría si se supiera que la red de Telefónica es tres veces más mala de lo que nos venden? Perderían clientes.
  - ¿Qué pasaría si se supiera que IBM tiene redes con tecnologías obsoletas? Darían muy mala imagen con respecto a la competencia.
  - ¿Qué pasaría si se supiera que la red de Orange da prioridad a las comunicaciones con origen en Telefónica que a las suyas propias? Los clientes de Orange se pasarían a telefónica.

BGP - Problemática gral. del encamin. Interdominio (y III)

- A modo de conclusión:
  - Nadie se fía de nadie.
  - Todos necesitan a todos, aunque unos más que otros.
  - Tener mucha conectividad implica tener mucho poder y dinero.
  - Todos tienen SÓLO una visión parcial de la topología de Internet.
  - No se puede llevar a cabo un encaminamiento basado en costes, porque se desconoce el coste dentro de la red del AS vecino.
  - Se debe llevar a cabo un encaminamiento basado en políticas para permitir por ejemplo: que una comunicación de IBM no pase por el AS de Intel, que una comunicación de la NASA no pase por un AS de Irak, que una comunicación desde España no pase por France Telecom para llegar a China (porque es más caro), etcétera.
  - La información de encaminamiento es oro. Debe llegar sólo a quien se desea.

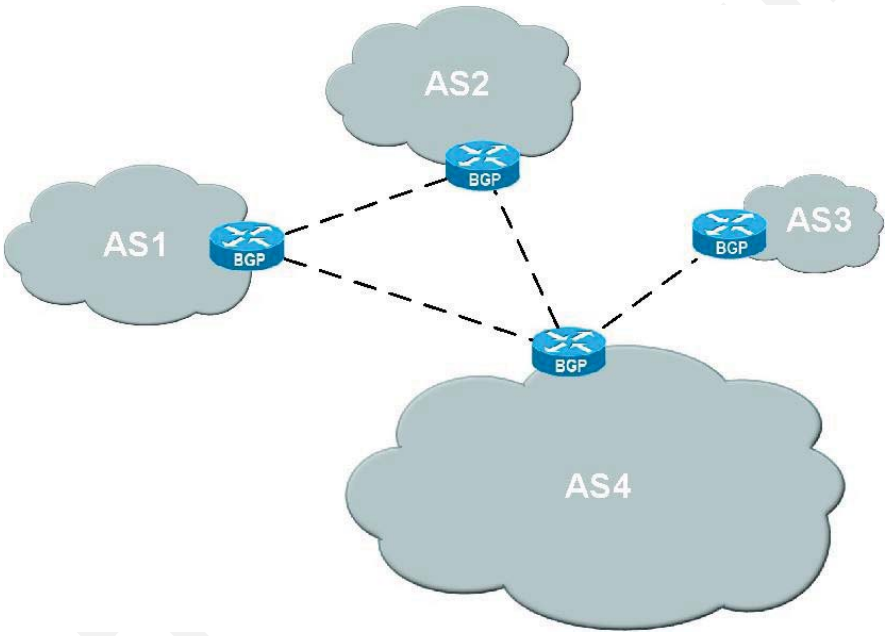
BGP - Evolución hasta BGP-4 (I)

- **Hace décadas:** los administradores de los AS se enviaban periódicamente un fichero de rutas para configurar de forma manual las rutas entre AS. Internet estaba formada por centros de investigación y era un entorno de confianza.
- **Posteriormente:** Internet crece de tamaño. Es complicado el mantenimiento manual. Aparece GGP *(Gateway to Gateway Protocol)*. Hay servidores de ruta en cada AS que intercambian las rutas entre ellos periódicamente.
- **Año 1984.** El IETF crea EGP *(Exterior Gateway Protocol)*. La explosión de Internet la convierte en un entorno no fiable. Hay que poder discriminar a quién se le ofrece información de encaminamiento y a quien no.
  - Cada AS sólo puede anunciar rutas que lleven a sus propias redes.
  - Tiene poca capacidad para aplicar políticas.
  - Tiene facilidad para crear bucles.
  - Entiende Internet como una red muy jerárquica.

BGP - Evolución hasta BGP-4 (II)

- **Año 1989:** el IETF genera el RFC de la primera versión de BGP. Comparte muchas ideas con EGP, en el que está basado. Pero corrige ciertos problemas encontrados:
  - Permite eliminar bucles.
  - Permite a un AS anunciar rutas propias así como las rutas aprendidas de terceros AS.
  - Permite aplicar políticas de encaminamiento más avanzadas.
- **Desde 1990 hasta la actualidad:** el IETF modifica BGP y libera las versiones 2, 3 y 4 (la actual) añadiendo al estándar del protocolo mejoras a problemas que han ido apareciendo con su uso y con la expansión de Internet:
  - Añade mejoras de escalabilidad y del tiempo de convergencia.
  - Añade características que lo acercan a la Internet real (menos jerarquizada de lo que suponía la primera versión).

BGP - Evolución hasta BGP-4 (y III)



BGP – Funcionamiento de BGP-4 (I)

- BGP es un protocolo de tipo *path-vector*. Esto significa que el protocolo mantiene tablas de rutas completas para llegar a un destino.
- La información de estas tablas es retransmitida a los nodos con los que se comparte información mediante un conjunto de mensajes BGP.
- Cada una de las rutas incorpora una serie de datos:
  - Red destino.
  - Conjunto de AS por los que hay que pasar para llegar a esa red.
  - Atributos de la ruta.
  - Otros datos menores.
- Las rutas son significativamente distintas a la información transmitida por los protocolos de encaminamiento interior. Por tanto, el modo de funcionamiento debe ser también distinto y los problemas asociados también son diferentes.

BGP – Funcionamiento de BGP-4 (II)

- Para compartir parte de las rutas de la tabla de encaminamiento con otros *routers* BGP, el protocolo cuenta con cuatro mensajes distintos:
  - Mensaje **OPEN:** se utiliza para establecer una sesión BGP con otro nodo BGP para compartir información de encaminamiento.
  - Mensaje **UPDATE:** se utiliza para hacer llegar información de encaminamiento de uno a otro nodo BGP: nuevas rutas, rutas que han dejado de ser válidas...
  - Mensaje **NOTIFICATION:** se utiliza para notificar situaciones de error.
  - Mensaje **KEEPALIVE:** sirve para mantener con vida una sesión BGP.
- ¡No existe un mensaje CLOSE! Cuando un nodo BGP cierra la sesión, esto provoca un mecanismo de actualización en cascada que puede afectar a todo Internet. Durante este proceso, la red es incoherente y el tráfico circulante se puede perder. Por ello una sesión sólo se cierra cuando hay un error irrecuperable o cuando un nodo BGP va a ser desactivado para siempre.

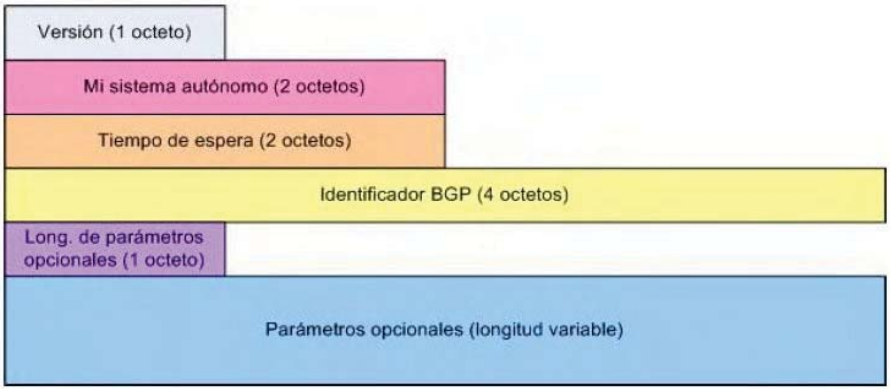
BGP – Funcionamiento de BGP-4 (III)

- Cabecera común a todos los mensajes BGP:

- **Marcador:** se incluye por compatibilidad hacia atrás.
- **Longitud:** tamaño en octetos del mensaje BGP. Cabecera incluida.
- **Tipo:** Número de 1 a 4 indicando si el mensaje es de tipo OPEN, UPDATE, NOTIFICATION o KEEPALIVE.

BGP – Funcionamiento de BGP-4 (IV)

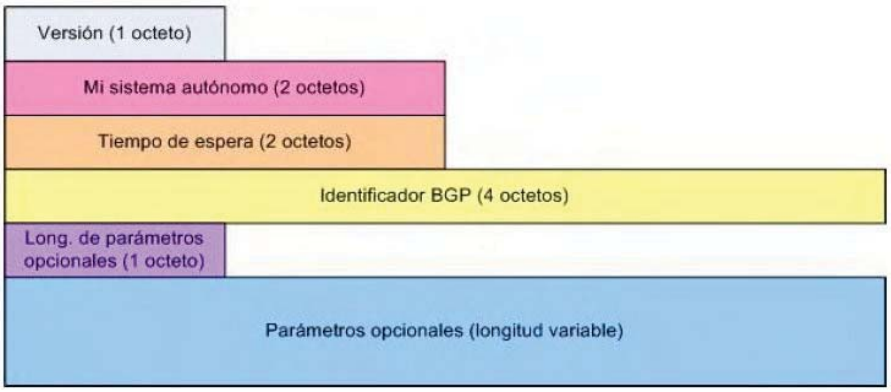
- Mensaje OPEN:



- **Version:** versión de BGP que se está usando.
- **Mi sistema autónomo:** número de AS al que pertenece el nodo BGP. Cada AS tiene un número asignado por el IANA *(Internet Assigned Number Authority)*.

BGP – Funcionamiento de BGP-4 (V)

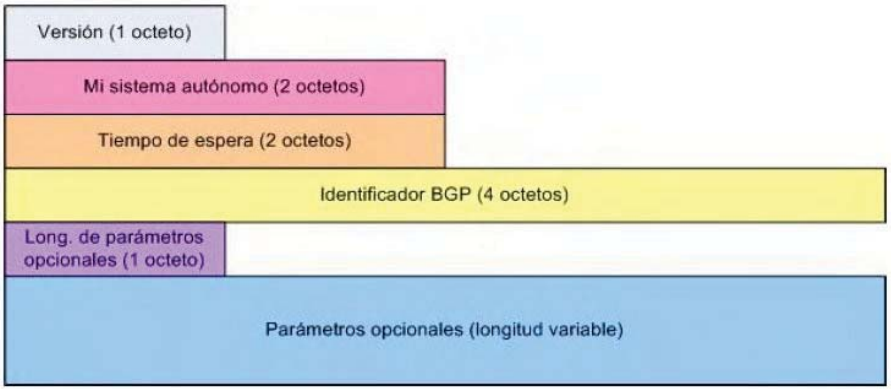
- Mensaje OPEN:



- **Tiempo de espera:** especifica el tiempo máximo que se espera sin tener noticias de la otra parte antes de cerrar la sesión BGP.
- **Identificador BGP:** número que identifica inequívocamente a un nodo BGP. Se suele usar una de las direcciones IP del nodo.

BGP – Funcionamiento de BGP-4 (VI)

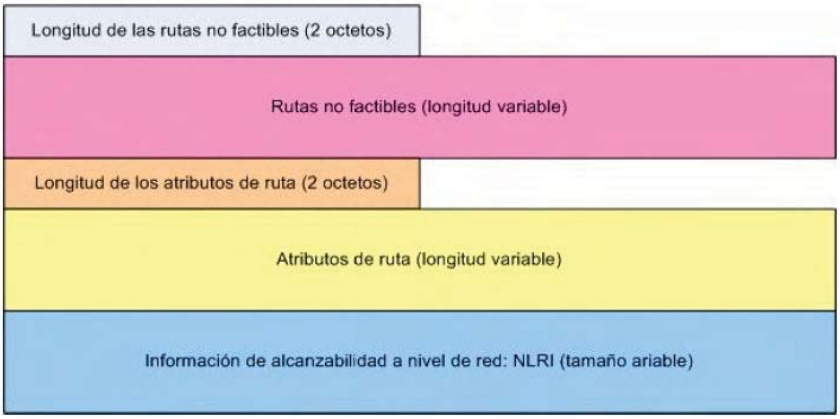
- Mensaje OPEN:



- **Longitud de parámetros opcionales:** tamaño en octetos del último campo.
- **Parámetros opcionales:** parámetros en formato TLV *(Type-Length-Value)* usados para negociar algunos aspectos durante la apertura de sesión.

BGP – Funcionamiento de BGP-4 (VII)

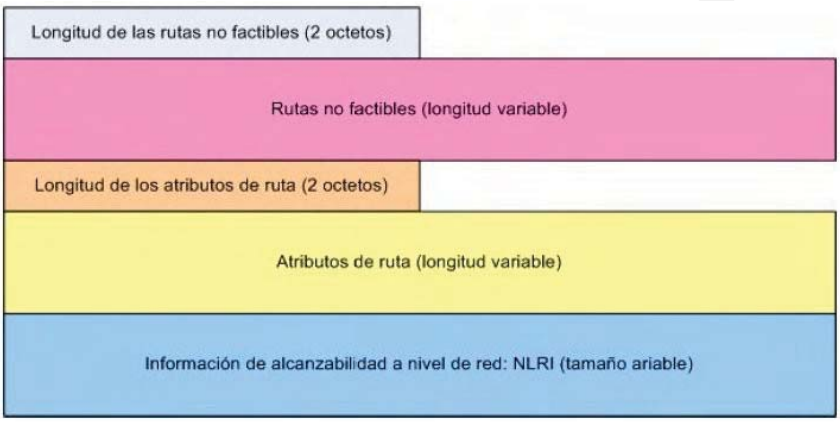
- Mensaje UPDATE:



- **Longitud de rutas no factibles:** longitud en octetos del 2º campo.
- **Rutas no factibles:** conjunto de destinos, en pares longitud-prefijo, que se deben anunciar a un vecino BGP como rutas "que dejan de serválidas".

BGP – Funcionamiento de BGP-4 (VIII)

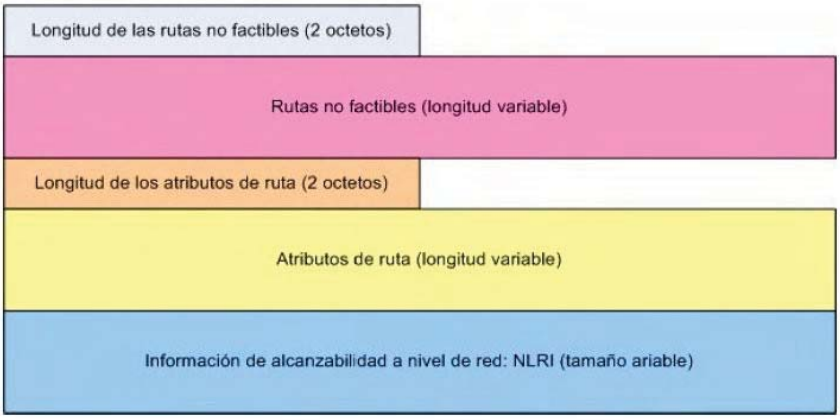
- Mensaje UPDATE:



- **Longitud de los atributos de ruta:** longitud en octetos del 4º campo.
- **Atributos de ruta:** conjunto de ternas TLV, que aportan información a la ruta que se anuncia; por ejemplo un identificador de AS por el que se pasa, origen, IP del siguiente salto, información para discriminar...

BGP – Funcionamiento de BGP-4 (IX)

- Mensaje UPDATE:



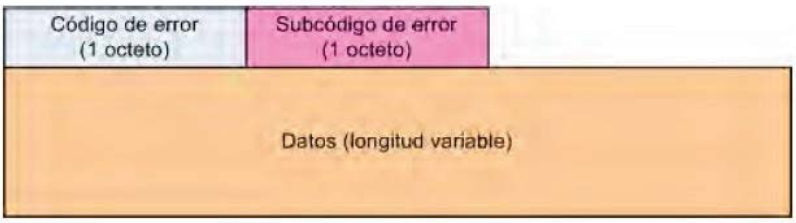
- **Información de alcanzabilidad a nivel de red NLRI:** indica la red o redes que se pueden alcanzar siguiendo la ruta especificada por los atributos de ruta. Esta información indica a un nodo BGP vecino que hay una nueva ruta disponible o que una ruta existente ha cambiado de atributos.

Nº 111

Administración Avanzada de Redes TCP/IP

BGP – Funcionamiento de BGP-4 (X)

- Mensaje NOTIFICATION:



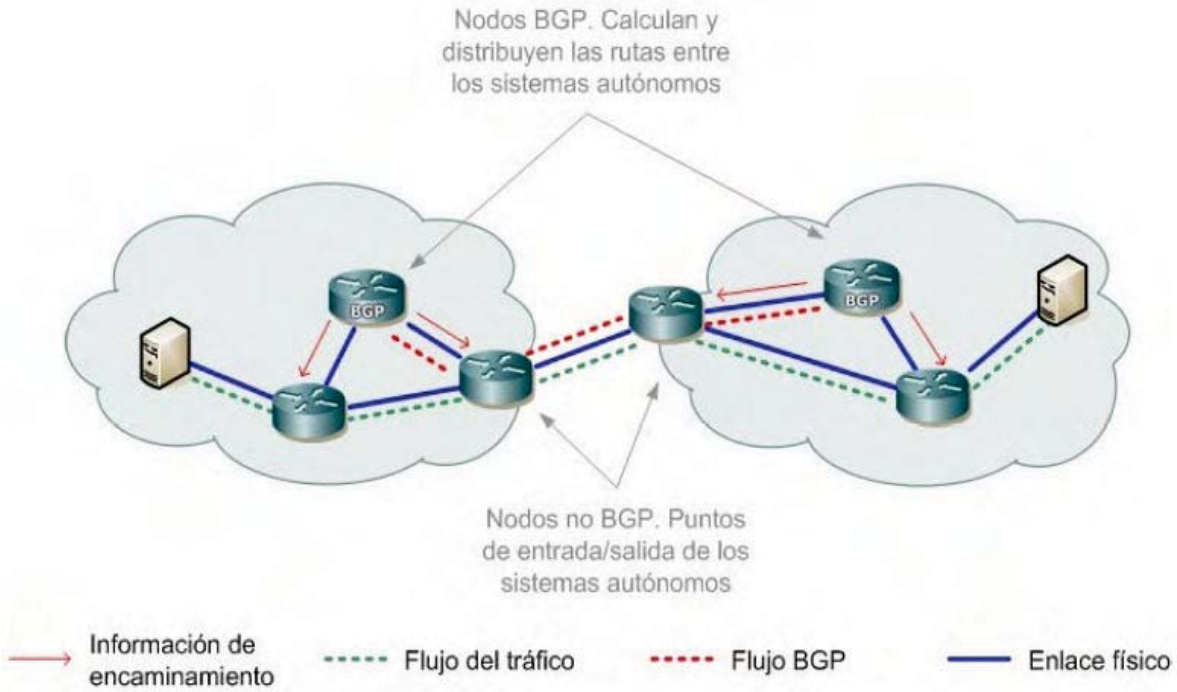
- **Código de error:** indica el tipo de error que ha generado el envío del mensaje y el cierre de la sesión BGP.
- **Subcódigo de error:** indica el subtipo de error que ha generado el envío del mensaje y el cierre de la sesión BGP.
- **Datos:** es un campo que puede existir o no. Si existe, contendrá tantos datos como sea posible para que el nodo BGP vecino pueda entender con más detalle que ha pasado, cómo debe adaptar su funcionamiento, etcétera.

Nº 112

BGP – Funcionamiento de BGP-4 (XI)

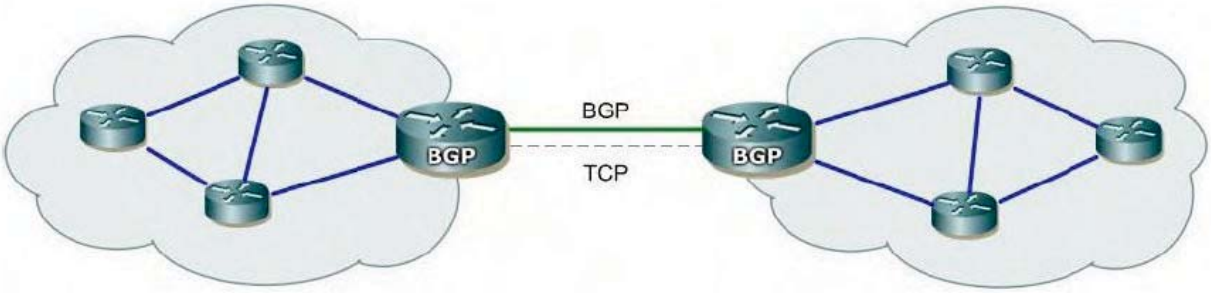
- Mensaje KEEPALIVE:
- El mensaje KEEPALIVE sólo está compuesto por la cabecera BGP en la que el mensaje se especifica como de este tipo.

BGP – Funcionamiento de BGP-4 (XII)



BGP – Funcionamiento de BGP-4 (XIII)

- Aunque BGP hace labores del nivel de red, realmente funciona sobre un protocolo de transporte; en la realidad, funciona sobre TCP.
- Para abrir una sesión BGP, primero se establece una sesión TCP entre los nodos BGP implicados, a través del puerto TCP 179.

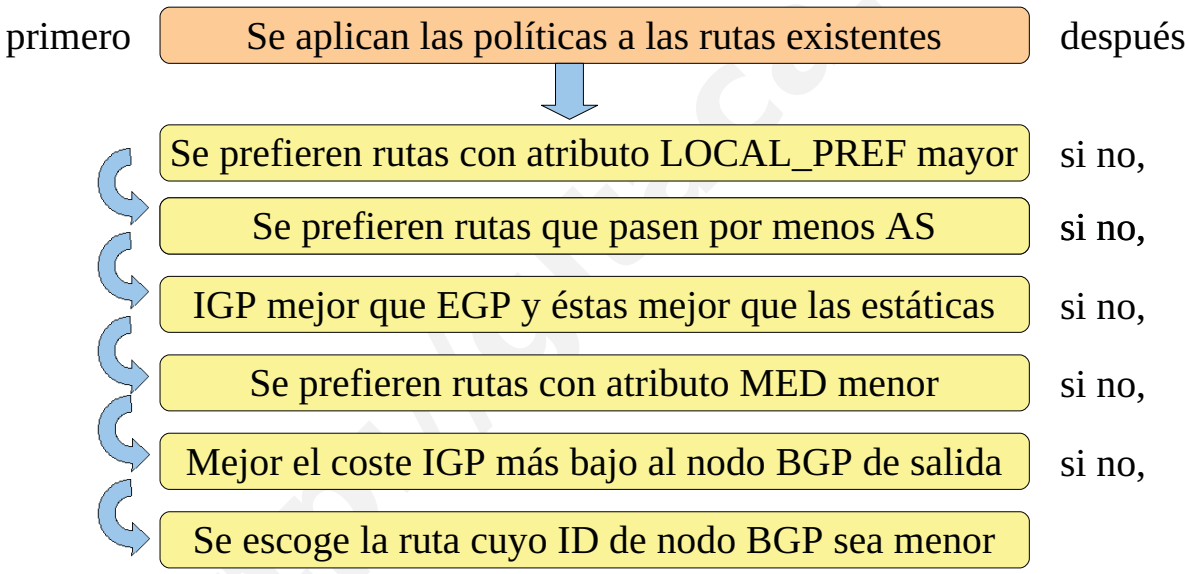


BGP – Funcionamiento de BGP-4 (XIV)

- Proceso de **selección de rutas**:
  - Un nodo BGP puede tener establecidas sesiones BGP con diversos nodos BGP vecinos; aunque las sesiones BGP siempre se establecen entre dos; ni más ni menos.
  - A un mismo nodo BGP pueden llegar distintas rutas conducentes al mismo destino (a la misma red o conjunto de redes). Entonces BGP realiza un proceso de selección donde, entre todas las disponibles, selecciona la más adecuada según su configuración.
  - Tras esto, inserta la ruta seleccionada en su tabla de encaminamiento y a partir de ese momento será la ruta que anunciará a sus vecinos.
  - Como siempre que se hace una selección, se pierde información. La ruta BGP seleccionada puede ser la mejor para un nodo BGP, pero no tiene por qué serlo para su vecino. Sin embargo, es la ruta que se le hará llegar.

BGP – Funcionamiento de BGP-4 (XV)

- Proceso de **selección de rutas**:

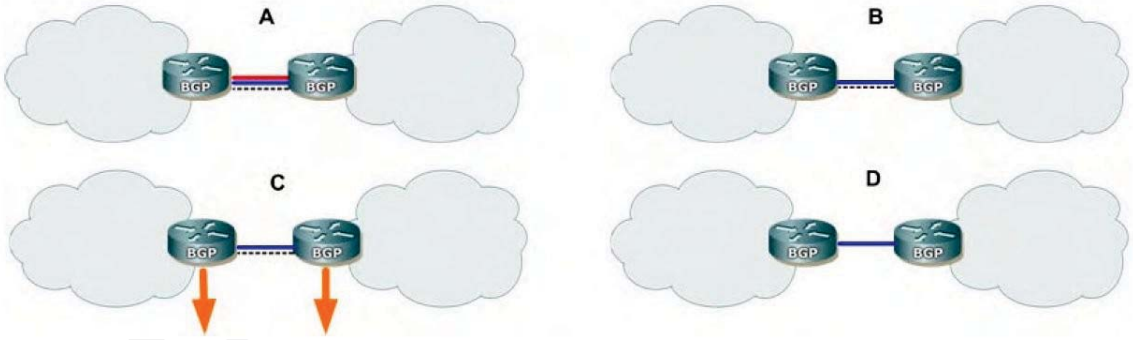


BGP – Funcionamiento de BGP-4 (XVI)

- Cuando un nodo BGP se conecta:
  - Se configura localmente.
  - Se establece una sesión TCP con el nodo BGP deseado.
  - Se manda mensaje OPEN para establecer la sesión BGP.
  - Se transmiten todas las rutas locales, una por una con UPDATE.
  - Se reciben todas las rutas del vecino, una por una con UPDATE.
  - Se intercambian de cuando en cuando mensajes KEEPALIVE, para mantener la sesión viva.
  - Cuando hay cambios, se intercambian UPDATES para mantener sus tablas de encaminamiento actualizadas.
  - ¿Para que valen estas rutas? Las rutas BGP son utilizadas cuando tráfico del AS propio debe llegar a alguna de las redes indicadas por dichas rutas. ¿Cómo? Gracias al atributo de ruta NEXT_HOP, que indica la IP del siguiente nodo a utilizar.

BGP – Funcionamiento de BGP-4 (XVII)

- Cuando se produce un error inesperado:
  - Se envía un mensaje NOTIFICATION para avisar del error (A).
  - Se cierra la sesión BGP automáticamente (B).
  - Se desechan todas las rutas asociadas a esa sesión (C).
  - Se cierra la conexión TCP sobre la que se sustentaba BGP (D).
  - Se propaga el efecto en cascada.

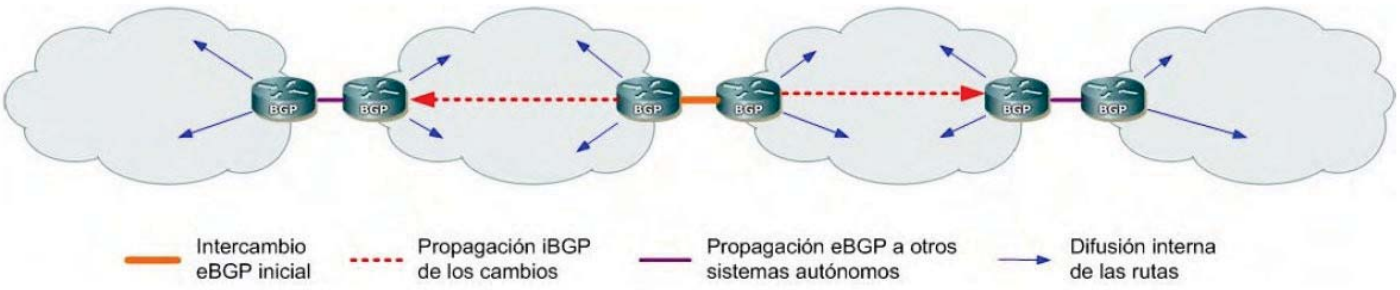


Nº 119

Administración Avanzada de Redes TCP/IP

BGP – Funcionamiento de BGP-4 (y XVIII)

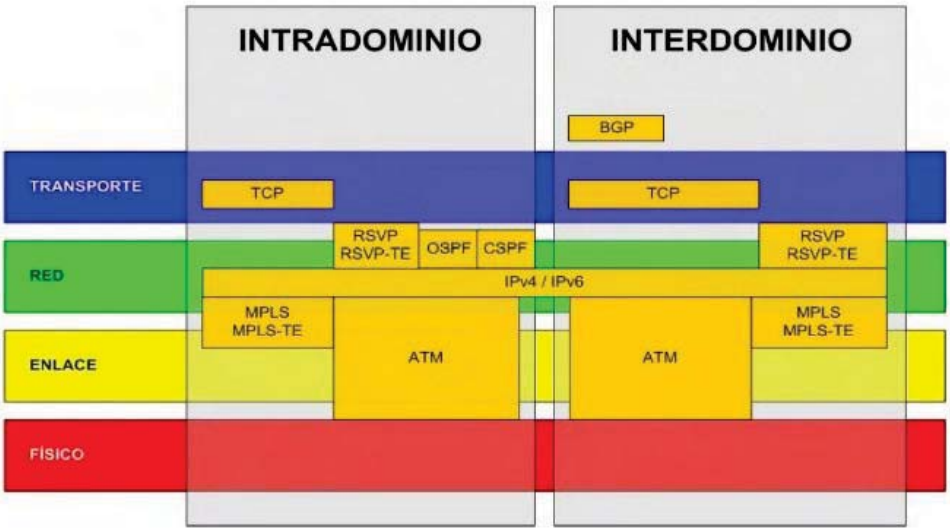
- Propagación en cascada.
  - Se produce un cambio que es anunciado al vecino BGP.
  - El vecino BGP actualiza sus tablas de rutas.
  - Si el vecino compartía esa ruta con otros AS, anuncia el cambio al nodo BGP de ese otro AS.
  - Este otro nodo realiza la misma operación.



Nº 120

BGP – Ubicación de BGP en la pila de protocolos TCP/IP

- BGP a nivel funcional: nivel de red.
- BGP a nivel de encapsulación: sobre el nivel de transporte.



Nº 121

Administración Avanzada de Redes TCP/IP

BGP – Problemática específica de BGP (I)

- BGP tiene muchos problemas que resolver en la actualidad. La mayoría de ellos, se pueden clasificar en tres tipos:
  - Problemas de **convergencia:** el tiempo de convergencia es aquel que tarda la red en ser coherente tras un cambio. El cambio producido por un mensaje UPDATE se propaga por toda la red. Mientras, la red es incoherente. El tiempo de convergencia debe tender a cero.
  - Problemas de **escalabilidad:** BGP tiene diversas restricciones que lo hacen escalar no demasiado bien. La mayor parte de ellas vienen dadas por el hecho de que un AS tenga más de una conexión otros AS vecinos.
  - Problemas de **ingeniería de tráfico:** para ingeniería de tráfico es importante tener el control de todos los lugares por los que va a circular el tráfico. En BGP no es sencillo.
  - En cualquier caso, todos los factores están interrelacionados, por lo que es complejo definir los límites en que se ve afectado BGP.

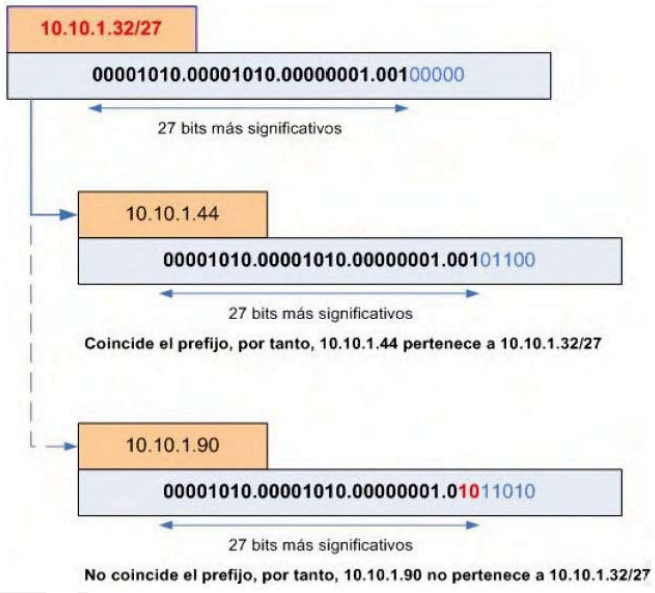
Nº 122

BGP – Problemática específica de BGP (II)

- Una tabla de rutas BGP a mediados de 2006 podía tener aproximadamente 180.000 rutas.
- Gran problema:
  - De memoria.
  - De recursos.
  - ¿Cuánto tarda en propagarse información de 180.000 rutas a través de Internet?
- **Problema: e**l número y tamaño de las rutas de en las tablas de encaminamiento inciden directamente en el tiempo de convergencia.
- **Objetivo:** disminuir el número de rutas a almacenar en las tablas.
- **Solución:** Agregación de rutas. Utilizar CIDR para abstraer los prefijos de red a uno superior.
- **Efecto colateral:** menos rutas implican menos capacidad para TE.

BGP – Problemática específica de BGP (III)

- Ejemplo de agregación de rutas.



BGP – Problemática específica de BGP (IV)

- **Problema:** el número y tamaño de las rutas de en las tablas de encaminamiento inciden directamente en el tiempo de convergencia. Sobre todos en nodos mal configurados que fallan y se recuperan con frecuencia. La red siempre está intentando converger.
- **Objetivo:** paliar los efectos nocivos de las oscilaciones producidas por este problema.
- **Solución:** *Route Flap Damping* (amortiguación de las oscilaciones de rutas). Se basa en mantener un temporizador en el nodo BGP que indica el intervalo mínimo que debe existir entre que se anuncia el cambio de una ruta y otro. Así, si se producen cambios muy seguidos, no se anuncian y se evita la oscilación.
- **Efecto colateral:** si el cambio es legítimo y no se produce por errores o fallos de configuración el nodo BGP, dicho cambio tarda más de la cuenta en ser anunciado.

BGP – Problemática específica de BGP (V)

- **Problema:** cuando una ruta deja de ser válida, hasta que este cambio llega a todos los nodos BGP de todos los AS implicados pasa un tiempo largo (decenas de minutos). Las rutas que ya no son válidas pero aún permanecen en los *routers* BGP en espera de ser eliminadas son **rutas fantasmas**. Estas rutas alargan el proceso de convergencia porque mientras estén ahí, esos *routers* las dan por buenas, las utilizan, las propagan como buenas...
- **Objetivo:** eliminar cuanto antes las **rutas fantasma**.
- **Solución:** *ghost flushing*. Es una técnica consistente en que los nodos BGP den prioridad a los mensajes UPDATE que llevan información sobre rutas no factibles (que dejan de ser válidad) y retarden, mediante *route flap damping*, los mensajes UPDATE que anuncian rutas válidas. Se reduce el tiempo de convergencia de minutos a segundos porque se elimina antes la información fantasma.

BGP – Problemática específica de BGP (VI)

- Cuando un AS tiene más de un nodo BGP para conectarse a más de un AS vecino, BGP requiere que estos nodos BGP, del mismo AS, estén conectados mediante una topología *full-connect* (todos con todos). Con dos o tres nodos BGP esto no es un problema. Pero cuando el número de nodos BGP asciende, este tipo de conexiones entre ellos no es escalable.
- **Problema:** el número de nodos de un mismo AS a interconectar asciende y la topología *full-connect* es inviable.
- **Objetivo:** minimizar el número de conexiones necesarias entre nodos BGP internos a un AS.
- **Solución:** *BGP Route Reflector* (BGP-RR). De puertas hacia fuera, un nodo es el encargado de mantener sesiones BGP con otros AS. Este nodo se encarga de retransmitir (reflejar) la información obtenida desde el exterior hacia los otros nodos BGP de su AS y viceversa. Estos otros nodos de su mismo AS se llaman clientes del *Route Reflector*.

BGP – Problemática específica de BGP (y VII)

- **Problema:** el número de nodos de un mismo AS a interconectar asciende y la topología *full-connect* es inviable.
- **Objetivo:** minimizar el número de conexiones necesarias entre nodos BGP internos a un AS.
- **Solución:** *BGP AS Confederations*. Se subdivide de forma interna un AS en varios AS. Desde fuera del AS, no se distingue este cambio. Desde dentro, no obstante, se aparcela el AS y se conectan mediante *full-connect* los nodos de cada parcela. De este modo, el número de conexiones entre nodos BGP de un mismo AS se reducen significativamente.
- **Efecto colateral:** realmente, aunque de puertas hacia fuera el AS aparezca como uno, el AS está dividido en varios sub-AS. Esto implica que una ruta que atraviese el AS deberá llevar un atributo AS_PATH por cada uno de estos sub-AS atravesados. Esto puede hacer que la selección de rutas sea distinta por usar *BGP AS Confederations*.

BGP – BGP en el mundo real (I)

- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.

Nº 129

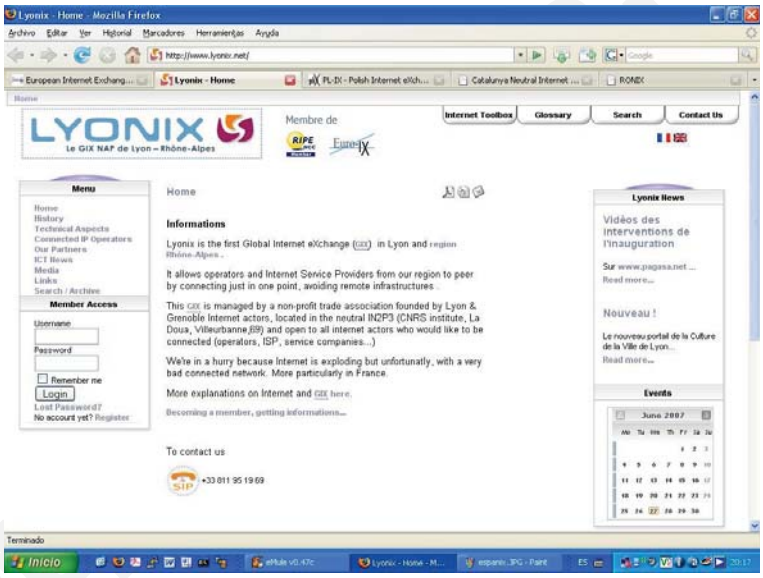
BGP – BGP en el mundo real (II)

- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.

Nº 130

BGP – BGP en el mundo real (III)

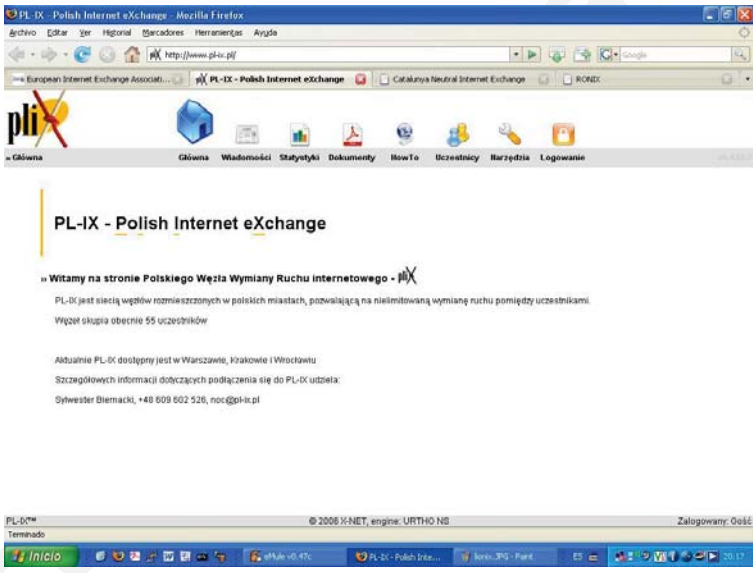
- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.



Nº 131

BGP – BGP en el mundo real (IV)

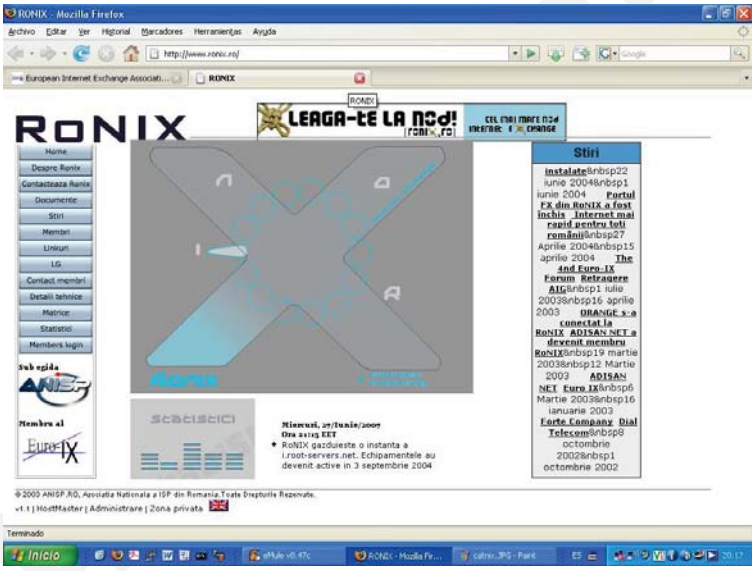
- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.



Nº 132

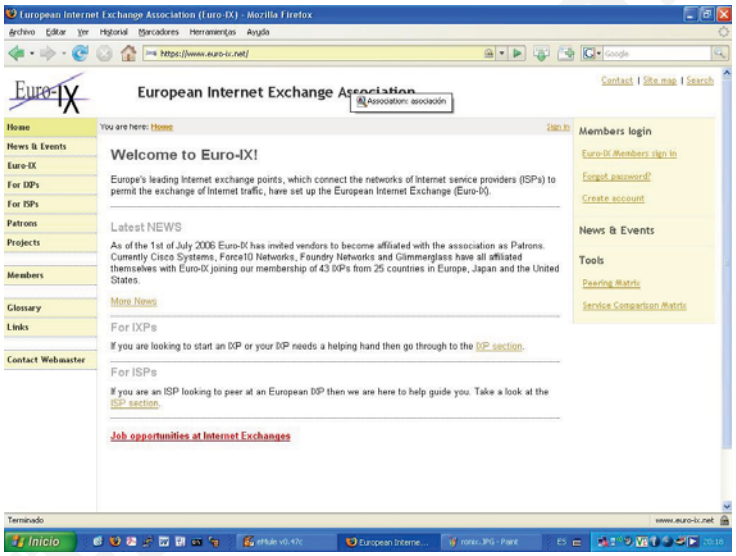
BGP – BGP en el mundo real (V)

- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.



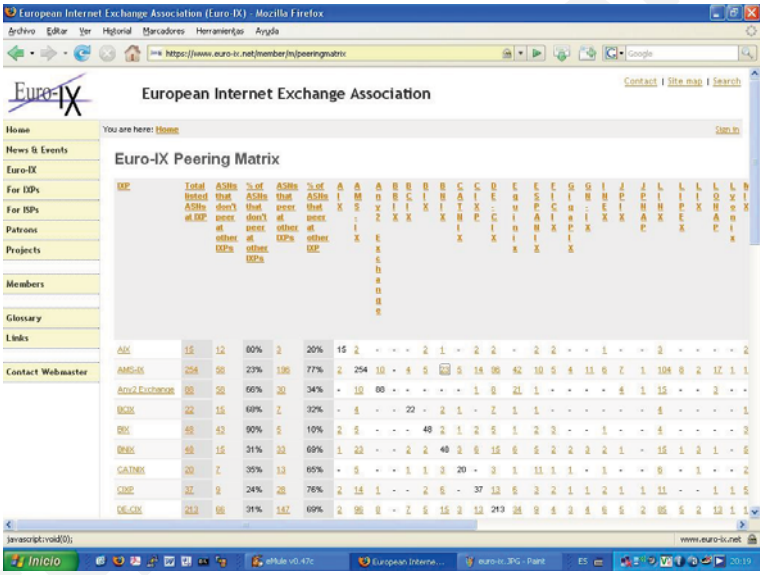
BGP – BGP en el mundo real (VI)

- **Puntos neutros:** puntos de la red donde se encuentran los nodos BGP de muchas compañías y donde se lleva un registro del *peering* entre AS.



BGP – BGP en el mundo real (VII)

- ***Peering matrix:*** representación en forma de matriz que expresa las relaciones de *peering* entre AS.



Nº 135

BGP – BGP en el mundo real (y VIII)

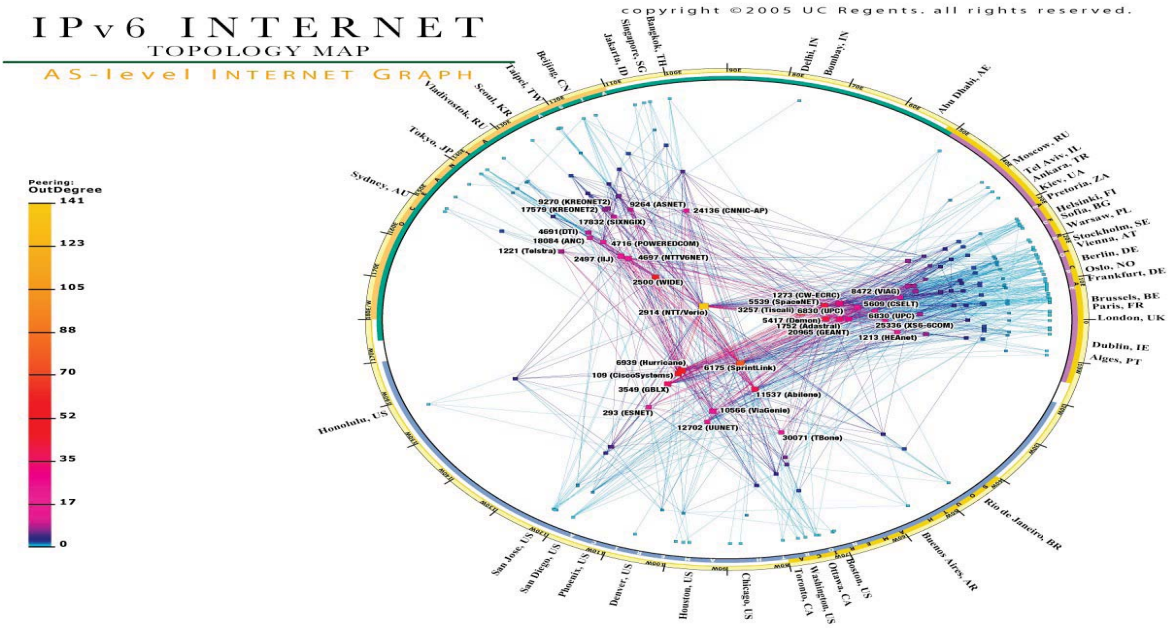
- Conclusión:

El acuerdo más importante de todos, el acuerdo de *peering*, se realiza al margen del protocolo BGP, como una negociación entre ISP. Un contrato.

- BGP comienza su funcionamiento SÓLO cuando este acuerdo formal se ha llevado a cabo.

Nº 136

4. IPv6 y versiones de TCP



Nº 137

Administración Avanzada de Redes TCP/IP

4) IPv6 y versiones de TCP

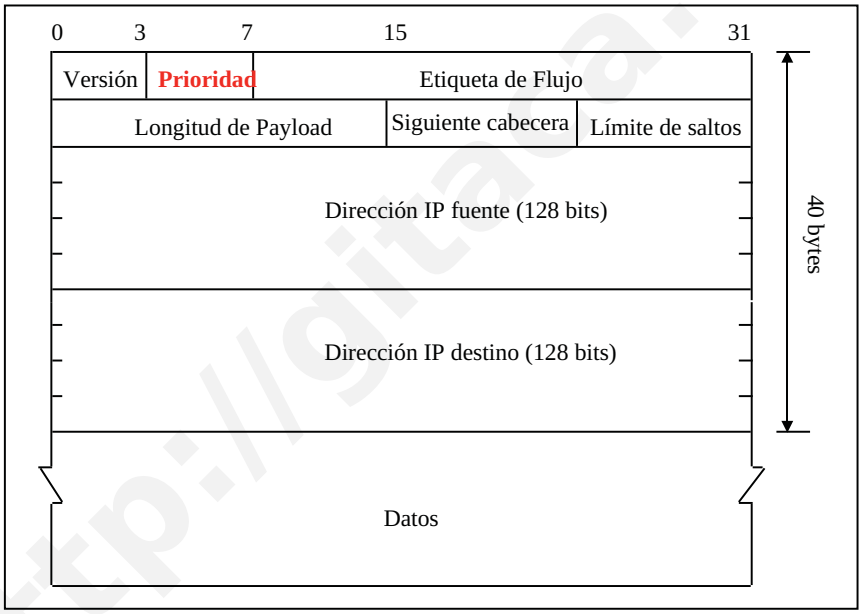
Objetivos

- Introducir la versión 6 de IP.
- Conocer el funcionamiento de TCP.
- Presentar las versiones de TCP más interesantes.
- Practicar con Network Simulator (ns).

Nº 138

4) IPv6 (Next Generation)

Prioridad: Distingue las fuentes a las que se puede controlar el flujo de info.
0-7 (fuentes capaces de controlar su flujo si hay

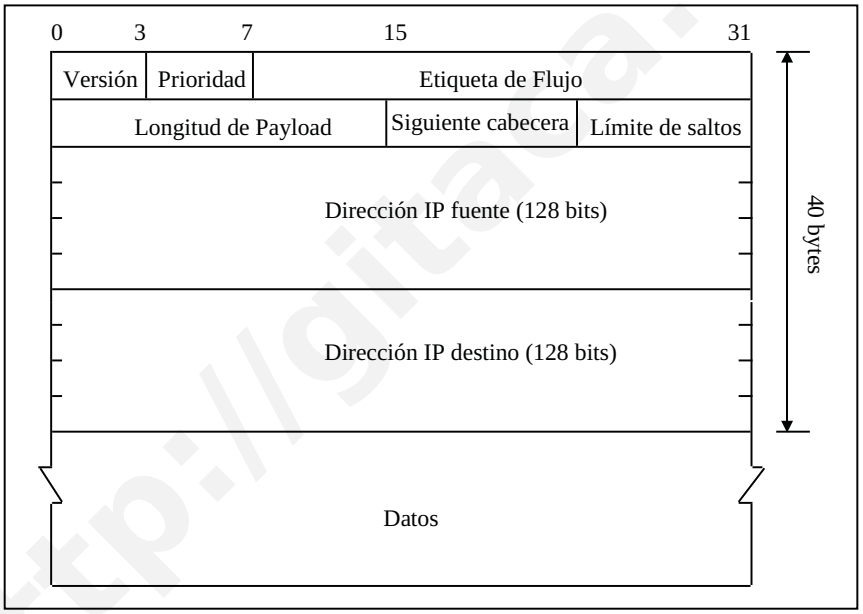


Nº 139

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

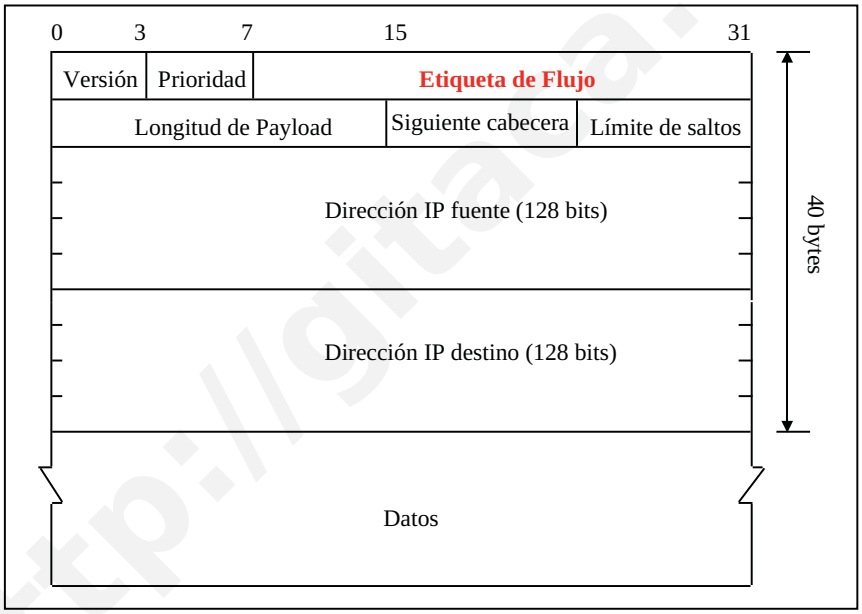
Congestión: 8-15 (para tráfico en tiempo real con velocidad constante (audio, video).



Nº 140

4) IPv6 (Next Generation)

Etiqueta de flujo: experimental y pensado para definir tipo de flujo concreto entre origen y destino.

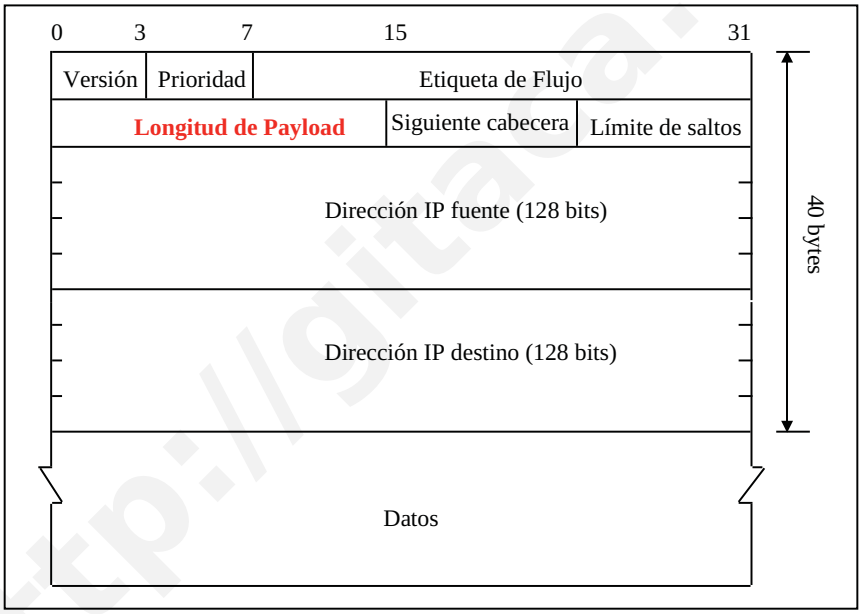


Nº 141

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

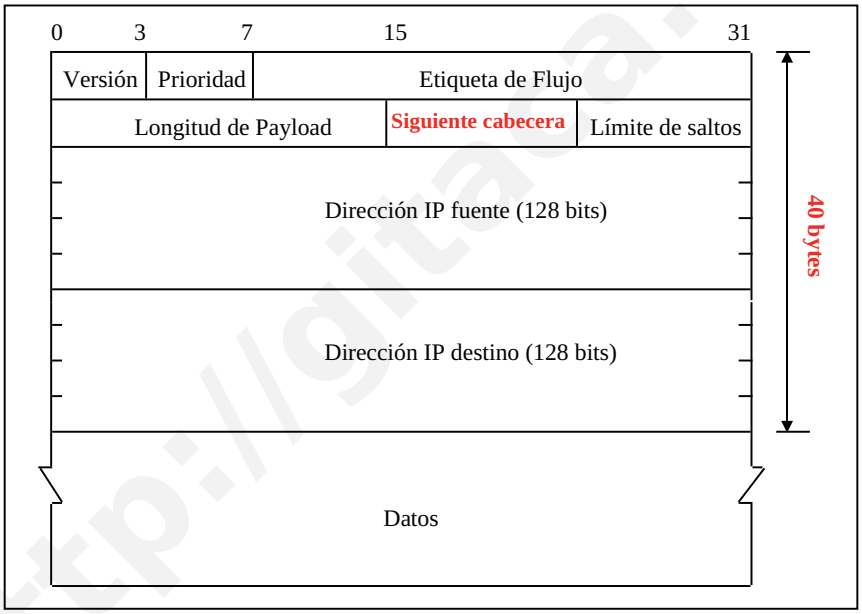
Longitud de carga útil: Cuántos bytes siguen a la cabecera de 40 octetos fijos.



Nº 142

4) IPv6 (Next Generation)

Siguiente cabecera adicional: 6 posibles cabeceras adicionales que simplifican las cabeceras. 8 bits que indican a routers si tras el datagrama viene alguna extensión u Opción. Sustituye el campo flags de IPv4 para no complicar la cabecera.



4) IPv6 (Next Generation)

Siguiente cabecera adicional: 6 posibles cabeceras adicionales que simplifican las cabeceras. 8 bits que indican a routers si tras el datagrama viene alguna extensión u Opción. Sustituye el campo flags de IPv4 para no complicar la cabecera.

<table>
<tr><td>Cabecera IPv6
(siguiente = TCP)</td><td colspan="3">Cabecera TCP + Datos</td></tr>
<tr><td>Cabecera IPv6
(siguiente = routing)</td><td>Cabecera Routing
(siguiente = TCP)</td><td colspan="2">Cabecera TCP + Datos</td></tr>
<tr><td>Cabecera IPv6
(siguiente = routing)</td><td>Cabecera Routing
(siguiente = Fragment)</td><td>Cabecera Fragment
(siguiente = TCP)</td><td>Fragmento
Cabecera TCP + Datos</td></tr>
</table>

Cadena de cabeceras en IPv6

4) IPv6 (Next Generation)

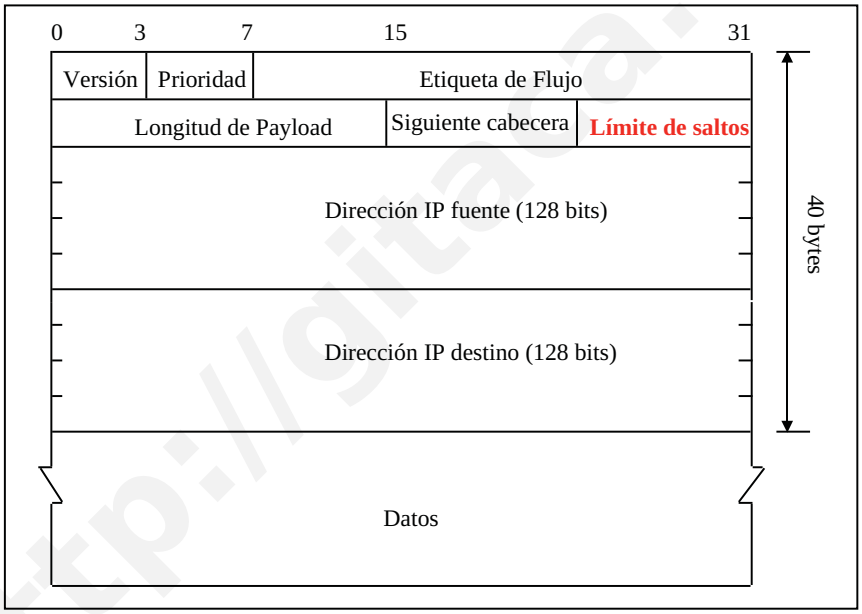
En IPv6 se definen una serie de cabeceras de extensión que se colocan justo después de los datos en forma de cadena (daisy chain) que permiten al usuario personalizar el tipo de datagrama, de forma que se puedan tener varias extensiones de cabecera indicando sólo en el campo siguiente cabecera de cada una el tipo de cabecera que viene a continuación.

Valor decimal	Abreviatura (keyword)	Descripción
0	HBH	Opciones entre saltos
4	IP	IP en IP (encapsulación en IPv4)
5	ST	Stream
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol
51	AH	Authentication Header
52	ESP	Encrypted Security Payload
59	NULL	No Next Header
60	DO	Destination Options Header
194	JBGR	Jumbogram

Algunos valores para los tipos de cabeceras en IPv6

4) IPv6 (Next Generation)

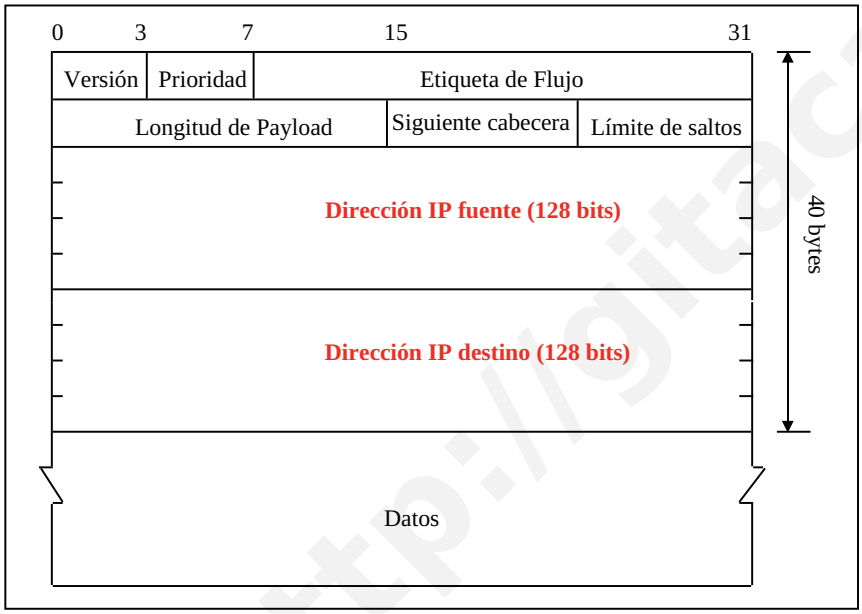
Límite de saltos: TTL de IPv4.



4) IPv6 (Next Generation)

Espacio de direcciones dividido en bloques:

0000 0000	IPv4
0000 001	OSI
0000 010	IPX
010	@ basadas en PSI
100	@ geográficas
.....	.....



Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

IPv6:

- Se pasa de 12 campos en IPv4 a 8 campos en las cabeceras de IPv6.
- En IPv6 los routers no fragmentan los datagramas. La fragmentación/ desfragmentación se hace extremo-extremo.
- Longitud total pasa a llamarse longitud de carga útil (payload length) permanece con tamaño de 16 bits (65.535 bytes).
- Protocolo pasa a llamarse Siguiente cabecera (netxt header) de 8 bits. Desaparece campo opciones pues en lugar de usar cabeceras de longitud variable se usan sucesivas cabeceras encadenadas.

4) IPv6 (Next Generation)

IPv6

- TTL pasa a llamarse límite de saltos (Hop limit) también de 8 bits.
- Clase de tráfico, también llamado Prioridad o Clase de 8 bits y equivalente a ToS
- Etiqueta de Flujo para permitir tráfico con requisitos de tiempo real (20 bits).
- La Clase y Etiqueta aportan las características fundamentales de IPv6: QoS y CoS y un poderoso mecanismo de control de flujo y de asignación de prioridades.

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

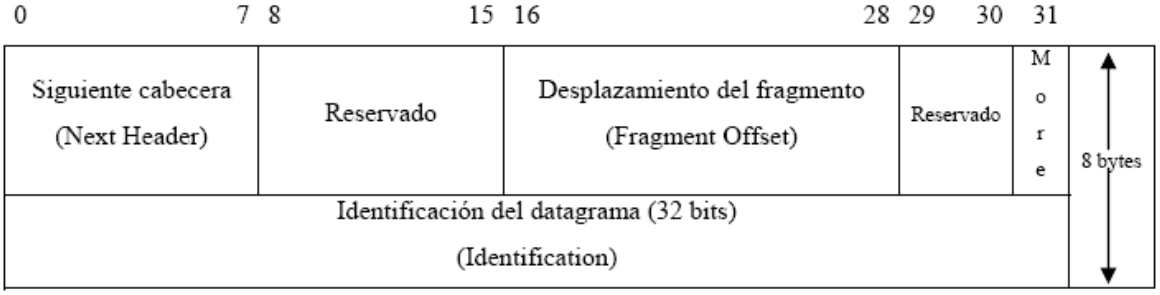
Cabecera de enrutamiento: 4 bytes a los que se añaden una serie de direcciones de 128 bits que corresponden a los routers por los que debe pasar el datagrama hasta llegar al destino

0 7	8 15	16 23	24 31
Siguiente cabecera (Next Header)	Tamaño de la cabecera (Header Extension Length)	Tipo de encaminamiento (Routing Type)	Segmentos restantes (Segments Left)
Dirección 1 (128 bits)			
.....			
Dirección N (128 bits)			

Cabecera de routing (tipo 0)

4) IPv6 (Next Generation)

Cabecera de fragmentación: En IPv6 no hay bit de fragmentación pues los datagramas no se fragmentan. Sirve para que la fuente (no routers intermedios) fragmente un tamaño superior al de MTU en varios fragmentos más pequeños.



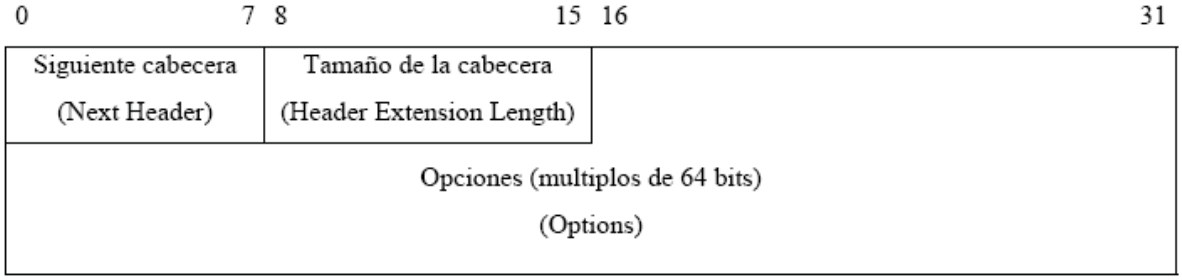
Cabecera de fragmentación de datagramas

Nº 151

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

Cabecera de opciones de destino: permite añadir opciones extra a los datagramas para que sean procesados sólo por el destinatario, así se permite que los routers intermedios que no necesitan interpretar las opciones puedan evitarlas sin perder tiempo de proceso.



Cabecera de opciones de destino

Cabecera de opciones entre destinos: permite especificar opciones que serán procesadas por todos los routers . Su formato es el mismo que el de las cabeceras de opciones de destino.

Nº 152

ICMPv2: Adaptado a IPv6

4) IPv6 (Next Generation)

0 – 7	8 – 15	16 – 23	24 – 31
Tipo (Type)	Código (ver 4-10) (Code)	Checksum	
Mensaje (Message body)			

Formato de la cabecera de ICMP v2 compatible con IPv6

Codigo	Significado
1	Destino inalcanzable (Destination Unrechable).
2	Datagrama demasiado grande (Packet too big).
3	Tiempo de respuesta agotado (Time Exceeded).
4	Parámetros incorrectos (Parameter Problem).
128	Solicitud de ECHO (ECHO Request).
129	Respuesta a ECHO (ECHO reply).
133	Solicitud de router (Router Solicitation).
135	Solicitud de vecino (Neighbour Solicitation).

Tabla de códigos más significativos de ICMP v2

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

Pseudocabeceras TCP y UDP compatibles con IPv6

0 – 7	8 – 15	16 – 23	24 – 31	
Dirección de origen (128 bits) (Source Address)				40 bytes
Dirección de destino (128 bits) (Destination Address)				
Tamaño de los datos (Payload Length)				
Campo nulo (Zero)			Siguiente cabecera (Next Header)	

Pseudocabecera de TCP y UDP compatible con IPv6

4) IPv6 (Next Generation)

Jumbogramas de IPv6

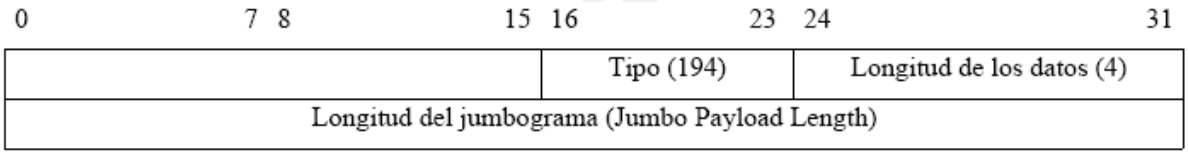
Tipo de red	Tamaño máximo de transacciones (MTU)
ATM	8192 bytes (para TCP/IP)
Comunicaciones punto a punto (PPP)	296 bytes
X.25	576 bytes
IEEE 802.3/ 802.2	1492 bytes
Ethernet	1500 bytes
FDDI	4352 bytes
Token Ring	4464 bytes
Fast Token Ring	17914 bytes
Hyperchannel	65535 bytes

MTU de las tecnologías de comunicaciones más extendidas

Administración Avanzada de Redes TCP/IP

4) IPv6 (Next Generation)

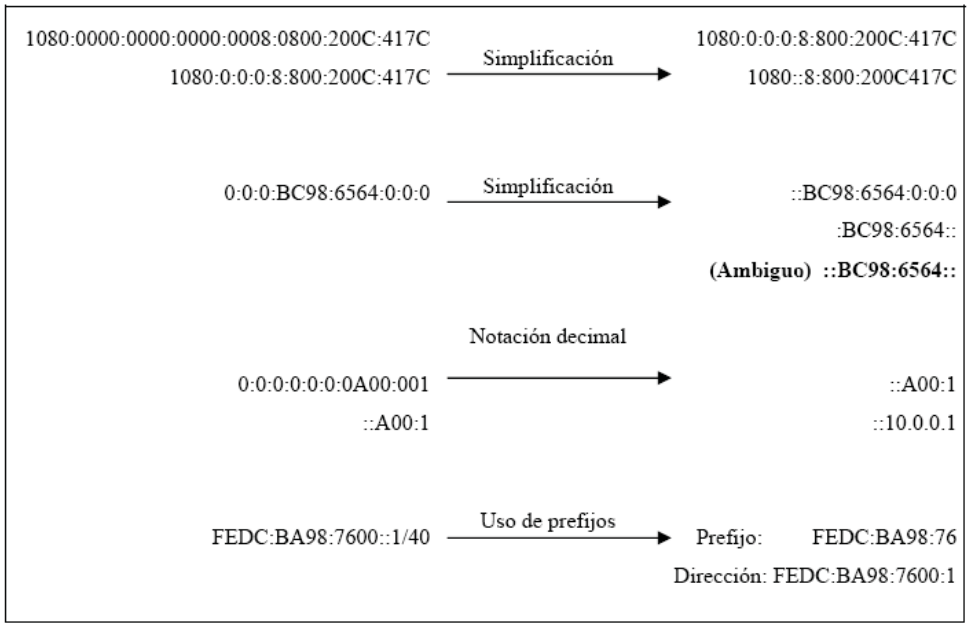
Jumbogramas de IPv6



Cabecera de un Jumbograma

Simplificación de direcciones de IPv6

4) IPv6 (Next Generation)



Simplificaciones del direccionamiento IPv6

Nº 157

4) TCP y sus implementaciones
Establecimiento de conexiones TCP

- Establecimiento de conexión a través protocolo *three-way handshake* (acuerdo de tres vías).

- *Server* espera pasiva de la llegada de una conexión entrante (*listen* y *accept*).

- *Client* ejecuta *connect* (@IP, puerto, tamaño segmento TCP que acepta, pwd, etc), esta primitiva envía un segmento con **SYN=1** y **ACK=0** y queda a la espera.

- Al llegar segmento al destino, se revisa si hay un proceso que haya ejecutado un *listen* en el puerto especificado:

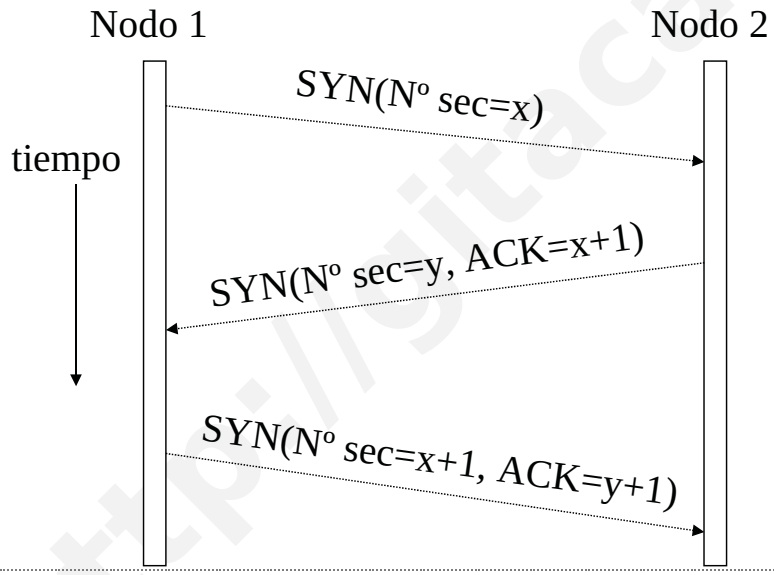
  - Si no lo hay se envía una respuesta con **RST=1** para rechazar la conexión.

  - Si algún proceso escucha en el puerto, ese proceso recibe el segmento y se acepta o rechaza la conexión. Si se acepta, se devuelve un segmento de ACK.

Nº 158

4) TCP y sus implementaciones

Establecimiento de conexiones TCP



4) TCP y sus implementaciones

Establecimiento de una conexión entre dos aplicaciones:

-Crear bloque de memoria para almacenar parámetros de TCP e IP (*socket*, Nº de secuencia, etc).

-Procedimiento de conexión con intercambio de mensajes (SYN y ACK). Cada parte informa a la otra de:

- Espacio libre en su buffer para recibir datos.
- Cantidad máxima de datos que puede llevar un segmento.
- Nº inicial de secuencia usado para numerar los datos de salida.

4) TCP y sus implementaciones

Pasos:

- Inicialización del servidor para aceptar conexiones de clientes (apertura pasiva).

- Cliente solicita apertura de conexión TCP con servidor para una @ y puerto IP especificado como apertura activa.

- TCP cliente envía segmento de sincronización SYN con Nº inicial de secuencia, tamaño de la ventana de recepción y tamaño del mayor segmento que puede recibir el cliente.

- TCP servidor envía otro SYN con Nº inicial de secuencia; un ACK con el identificador del primer byte de datos que debería enviar el cliente; tamaño de su ventana de recepción y tamaño del mayor segmento datos que puede recibir.

Administración Avanzada de Redes TCP/IP

4) TCP y sus implementaciones

Pasos:

- Al llegar al TCP cliente el mensaje SYN/ACK del servidor, envía de vuelta un ACK con Nº que debería tener el primer byte de datos enviado por el servidor.

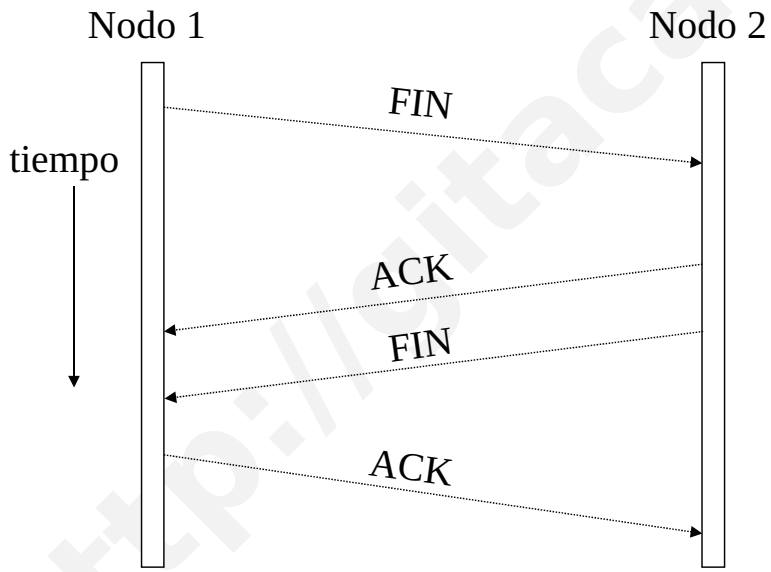
- Tras enviar el ACK, el TCP cliente informa a su aplicación que la conexión está abierta.

- El TCP servidor recibe el ACK del TCP cliente e informa también a su aplicación que la conexión está abierta.

Hecho todo esto, cliente y servidor están listos para el intercambio de datos.

4) TCP y sus implementaciones

Liberación de conexiones TCP



4) TCP y sus implementaciones

Terminación de una conexión:

Este proceso puede ser provocado por cualquiera de las partes. Suponiendo que es la aplicación servidora la que inicia el proceso:

1.- Aplicación servidora indica a TCP que termine la conexión.

2.- TCP servidor envía segmento final para informar a cliente que no enviará más datos.

3.- El TCP cliente envía un ACK del segmento final anterior.

4) TCP y sus implementaciones

Terminación de una conexión:

Este proceso puede ser provocado por cualquiera de las partes. Suponiendo que es la aplicación servidora la que inicia el proceso:

4.- TCP cliente informa a aplicación cliente que servidor desea terminar.

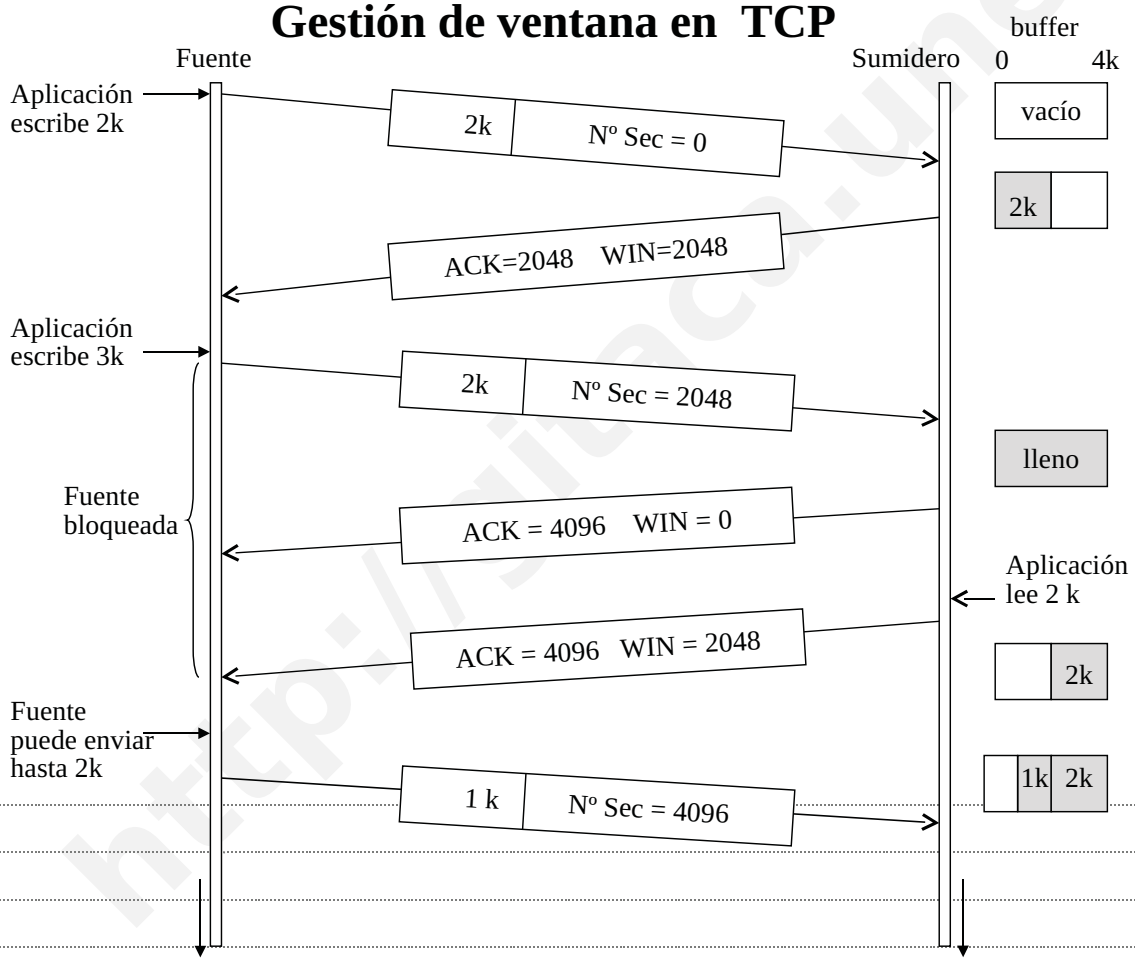
5.- Aplicación cliente indica a TCP que termine.

6.- TCP cliente envía segmento final.

7.- TCP servidor responde con ACK al recibir el segmento anterior.

8.- TCP servidor informa finalmente a su aplicación que la conexión ha terminado.

Gestión de ventana en TCP



Gestión de ventana en TCP

Si ventana anunciada por el receptor es 0, la fuente no puede enviar segmentos, salvo:

- Que se envíen datos urgentes (matar un proceso, mensaje, etc).
- Emisor envíe un segmento de 1 byte para que el receptor reanuncie el siguiente byte esperado y el tamaño de ventana. Evita bloqueos por pérdida de anuncio de la ventana.

No es necesario que fuentes envíen datos tan pronto como llegan de la aplicación, ni que los receptores envíen ACK tan pronto como sea posible. Objetivo: emisor no envíe segmentos pequeños y que el receptor no los pida:

- Algoritmo de Nagle: Envío de un byte cada vez. Se envía el primer byte en un segmento y el resto se entra en un buffer hasta que llegue el ACK del primer byte.
- Síndrome de ventana tonta (Clark). Emisor transmite bloques muy grandes, pero la aplicación receptora lee 1 byte cada vez. Se intenta que el receptor anuncie ventanas lo más grandes posible: mínimo de (tamaño máximo de segmento anunciado al inicio de la conexión, buffer vacío a la mitad).

4) TCP y sus implementaciones

Conceptos

• SEGMENTO. Se utiliza para designar cualquier paquete TCP, ya sea un paquete de datos o uno de reconocimiento (Ack).

• RWND (*Receiver Window*): es la cantidad máxima de datos que puede recibir un receptor de trafico TCP.

• CWND (*Congestion Window*): La ventana de congestión es una variable que limita la cantidad de datos que TCP puede enviar (en ningún momento TCP podrá enviar segmentos con un número de secuencia mayor que la suma del ACK con mayor número de secuencia recibido y el menor de los tamaños de las variables *rwnd* y *cwnd*). Su tamaño variará dependiendo de las condiciones de la red, si la red no descarta paquetes, el tamaño de la ventana aumentará, aumentando la velocidad de transmisión del receptor.

4) TCP y sus implementaciones

Conceptos

- SMSS (*Sender Maximum Segment Size*) Es el mayor tamaño de un segmento que el emisor puede transmitir. La cantidad máxima de datos que el emisor puede enviar.
- RMSS (*Receiver Maximum Segment Size*) Es el mayor tamaño de segmento que el receptor puede admitir. La cantidad máxima de datos que el receptor puede recibir.
- IW (*Initial Window*) Valor inicial que toma la ventana de congestión.
- RTT (*Round Trip Time*) tiempo que transcurre desde que el segmento ha sido enviado, hasta que se recibe la confirmación de que ha sido recibido por el receptor. El RTT determina la velocidad de transmisión de TCP, ya que el emisor TCP envía cada RTT el tamaño determinado por *cwnd*.

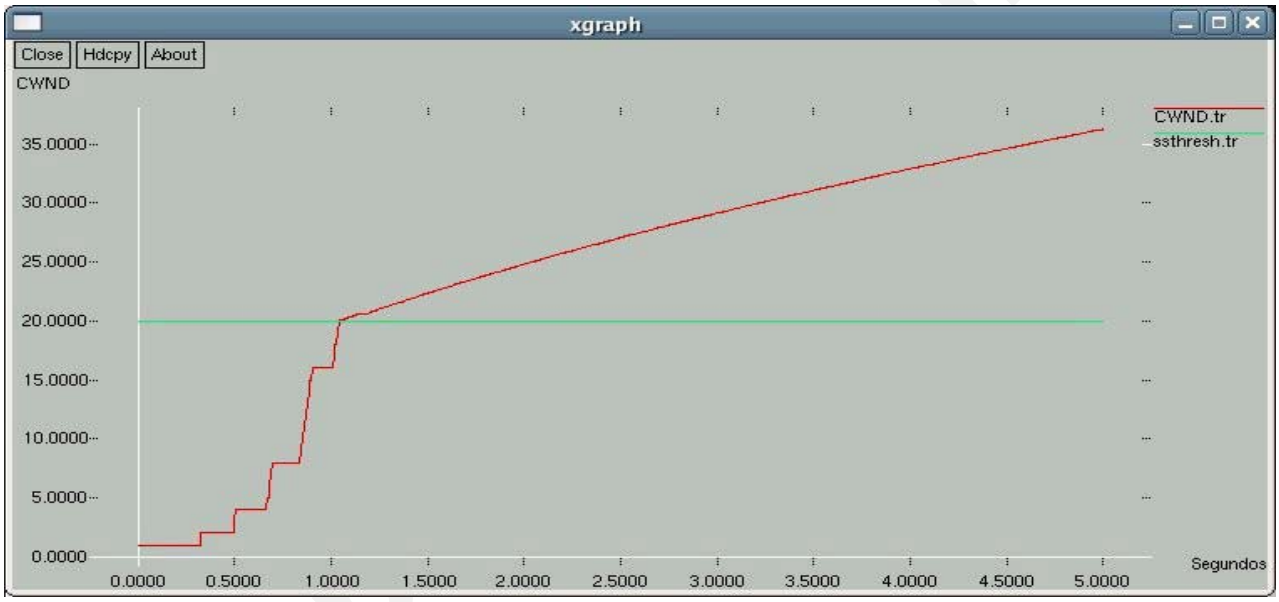
4) TCP y sus implementaciones

Conceptos

- CURRENT WINDOW representa la cantidad de información que envía el emisor cada RTT. Esta ventana toma el valor más pequeño entre CWND y RMSS.
- SSTHRESH. Esta variable se utiliza para determinar qué algoritmo de control de congestión, *Slow Start* o *Congestion Avoidance* se debe utilizar:

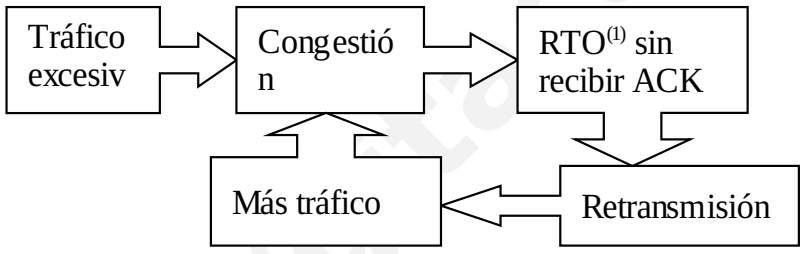
Si cwnd ≤ ssthresh	Usar *Slow start*
Si cwnd > ssthresh	Usar *Congestion avoidance*

4) TCP y sus implementaciones



4) TCP y sus implementaciones

Control de flujo

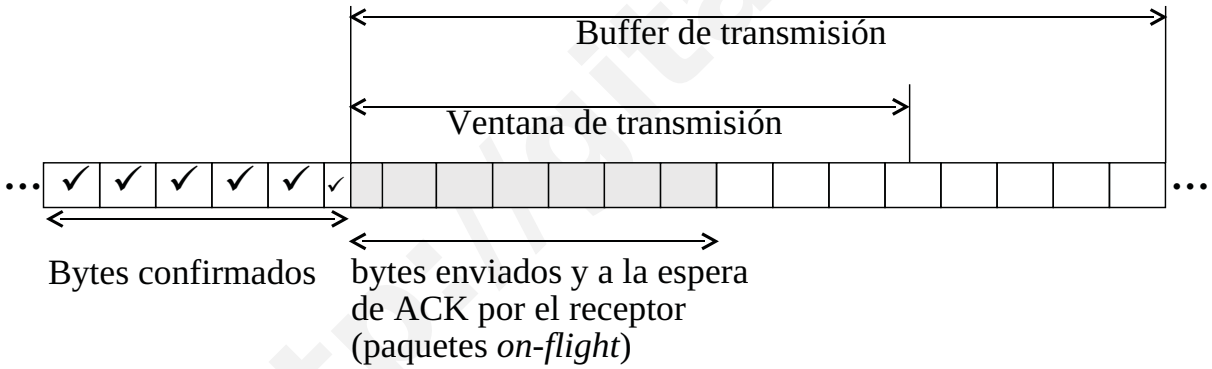


(1) RTO: *Round Trip Overtime*. Tiempo que se espera la recepción de la confirmación de un paquete (ACK).

4) TCP y sus implementaciones

Control de flujo (mecanismo de ventana deslizante)

Ventana de transmisión

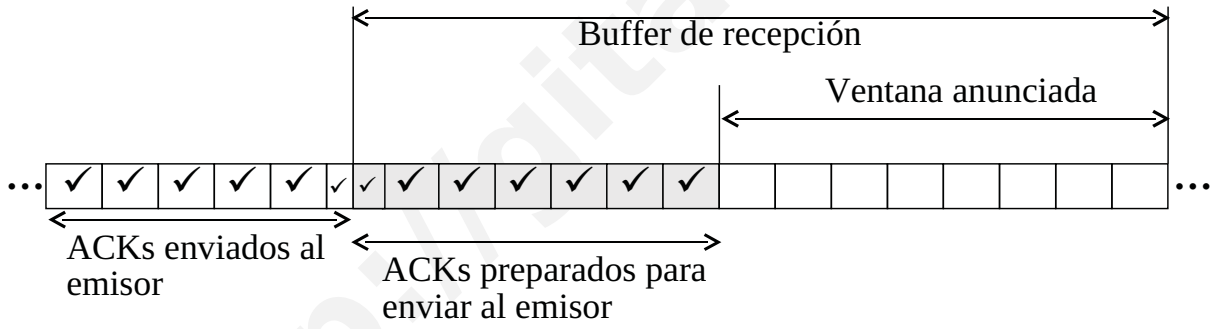


Administración Avanzada de Redes TCP/IP

4) TCP y sus implementaciones

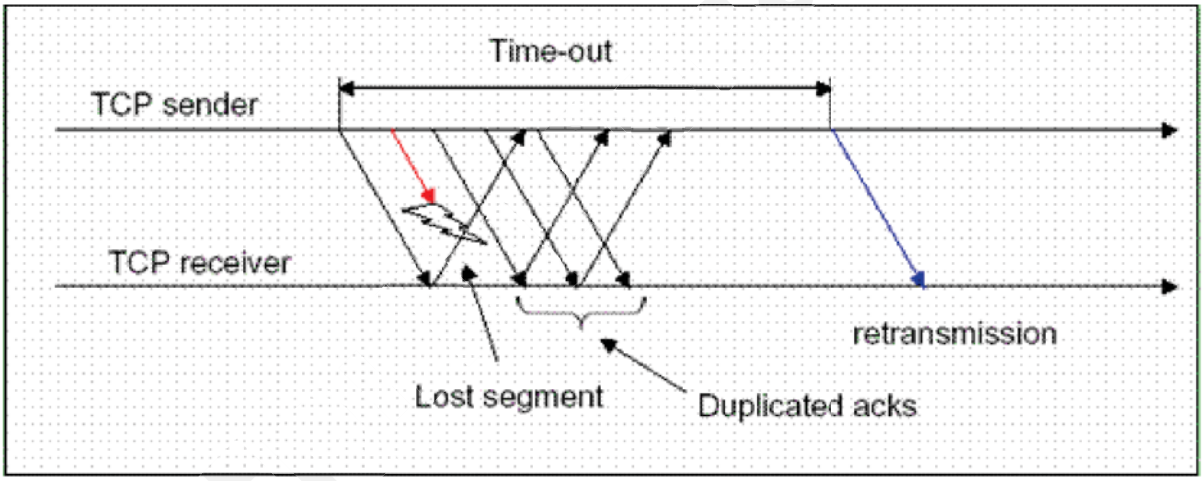
Control de flujo (mecanismo de ventana deslizante)

Ventana de recepción



4) TCP y sus implementaciones

Mecanismo de control de flujo y recuperación de paquetes en TCP



4) TCP y sus implementaciones

Control de congestión en TCP

- Cuando la carga de la red es superior a lo que puede soportar.

- Capa de red también puede manejar las congestiones, pero la tarea dura le corresponde a TCP, ya que la solución real consiste en la disminución de la tasa de datos.

- Ley de conservación de los paquetes: un paquete entra en la red sólo cuando ha salido otro de ella. Lograrlo mediante una gestión dinámica del tamaño de la ventana.

- Primer paso: detección de la congestión. Un temporizador puede actuar por pérdida de paquete debida a: ruidos o descarte por congestión. Los errores son poco frecuentes y lo más habitual son las congestiones.

4) TCP y sus implementaciones

Control de congestión en TCP

- En el establecimiento el receptor especifica un tamaño de ventana basado en su tamaño de buffer. Si la fuente se ajusta a este tamaño de ventana no habrá desbordamientos de buffer en el receptor, pero sí pueden aparecer en la red.

- Símiles hidráulicos con Internet: dos problemas: capacidad de la red y del receptor manejadas por separado en Internet.

- Cada transmisor usa dos ventanas: la que le ha especificado el receptor y la ventana de congestión. Cada una refleja la cantidad de bytes que puede enviar el emisor. El volumen de datos a enviar es la menor de las dos ventanas.

- Al establecerse la conexión el emisor asigna a la ventana de congestión el tamaño de segmento máximo usado por la congestión, y envía un segmento máximo.

Administración Avanzada de Redes TCP/IP

4) TCP y sus implementaciones
Control de congestión en TCP

- Si se recibe el ACK de este segmento antes de acabar el temporizador, el emisor aumenta el tamaño de la ventana de congestión al número de bytes de dos segmentos y envía dos segmentos.

- Cuando se reciben los ACK de esos dos segmentos se aumenta la ventana en otros dos segmentos. Cada ráfaga de segmentos reconocida con ACK duplica el valor del tamaño de la ventana de congestión.

- La ventana de congestión sigue creciendo exponencialmente hasta que salta un temporizador o se alcanza el tamaño de la ventana receptora. Si una ráfaga de segmentos (4096) provoca el salto de un temporizador, hará que la ventana de congestión se ajuste a la mitad (2048) de bytes de la ráfaga que provoca el *time-out*. Mientras la ventana de congestión esté en 2048 no se enviará una ráfaga de mayor longitud, sin atender a la ventana admitida por el receptor. Este algoritmo se llama Slow Start (arranque lento), aunque es exponencial.

4) TCP y sus implementaciones

Control de congestión en TCP

- El algoritmo de control de congestión usa, además de las ventanas de congestión y de recepción, un tercer parámetro umbral (inicialmente de 64 K).

- Cuando salta el temporizador se ajusta el umbral a la mitad de la ventana de congestión actual y la ventana de congestión se reinicia a 1 segmento.

- Por tanto, el Slow Start se usa para determinar lo que la red puede soportar hasta que el crecimiento exponencial se detiene por alcanzar el umbral.

4) TCP y sus implementaciones

Control de congestión con TCP

- A partir de ese momento las transmisiones exitosas aumentan linealmente la ventana de congestión (un segmento por ráfaga en lugar de un segmento por cada segmento).

- Si salta un temporizador se fija el umbral a la mitad de la ventana actual y se inicia de nuevo el Slow Start. Llegará de nuevo a alcanzar el umbral hasta que la ventana de congestión aumente linealmente. Si no hay time-outs la ventana de congestión continúa creciendo hasta el tamaño de la ventana del receptor. Aquí deja de crecer y permanece constante mientras no haya más time-outs y la ventana del receptor no cambie de tamaño.

- Mayoría de pérdidas son debidas a congestiones.

Algoritmo Slow-Start (S-S)

- TCP en redes WAN.

- Consulta y detecta el estado de la red para adecuar el tráfico TCP.

- Comienzo de transmisión lento para aumentar gradualmente (exponencial).

- Variable CWND limita la cantidad de segmentos que puede enviar la fuente para no inundar (congestionar) la red y/o al receptor.

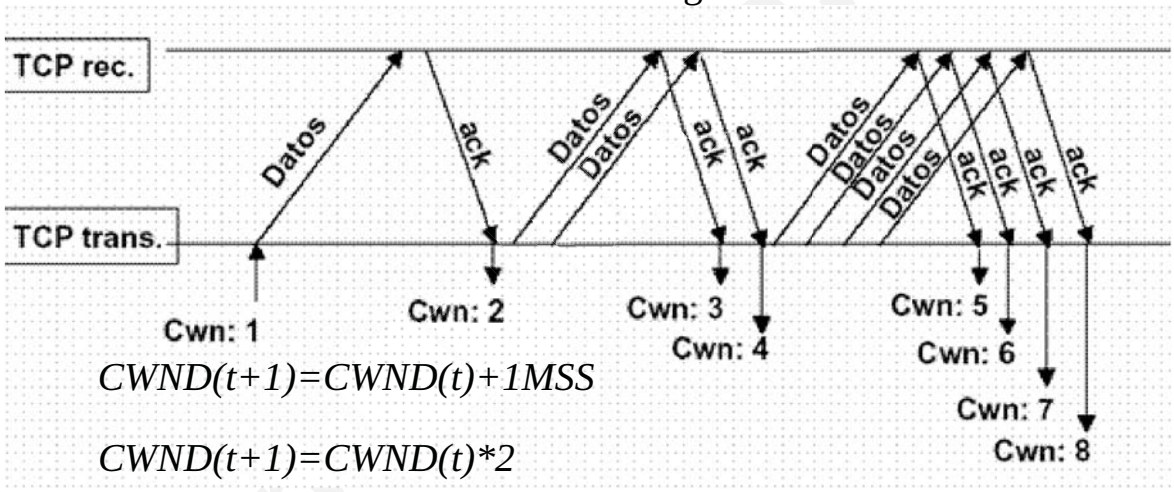
-Valor de CWND=1 negociado inicialmente entre emisor y receptor. Por cada ACK recibido en el emisor aumenta en 1 segmento el tamaño de CWND mientras sea menor que la de recepción (cuyo valor es normalmente rápidamente alcanzado).

- La fuente coloca segmentos en la red a la velocidad que recibe los ACK.

Administración Avanzada de Redes TCP/IP

Algoritmo Slow-Start (S-S)

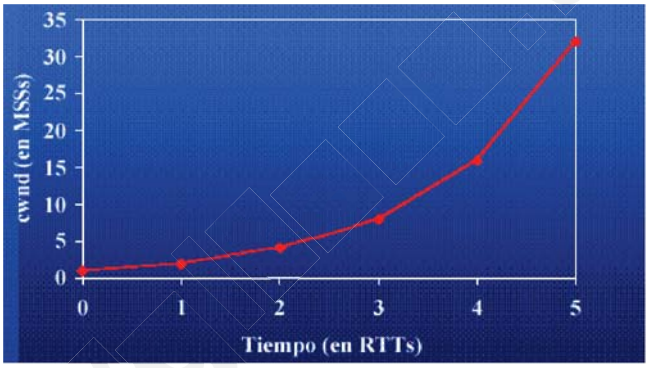
Evolución del tamaño de la ventana de congestión CWND en S-S



Nº segmentos enviados cada RTT usando la ventana CWND crece exponencialmente

Algoritmo Slow-Start (S-S)

Evolución del Nº de segmentos enviados cada RTT



-A mayor congestión, menos ACK recibidos y por tanto CWND más pequeña.

- El envío exponencial de los segmentos se mantiene mientras:
  - CWND<RWND
  - CWND ≤ SSTHRESH
  - No exista congestión

Administración Avanzada de Redes TCP/IP

Algoritmo Slow-Start (S-S)

- En ausencia de congestión se alcanza RWND en RTT*$\log_2$(RWND) segundos.

- S-S hace oscilar la CWND en torno a su valor ideal ajustando la velocidad a la que se deben transmitir los datos.

- S-S pone a prueba la capacidad de la red mediante el aumento progresivo del ritmo de envío de datagramas hasta detectar congestión.

- Agresivo pues no reduce tamaño ventana hasta perder paquetes. Por ello se combina con otros algoritmos. Primero hay que averiguar a qué ritmo pueden enviarse datos (S-S). Cuando ritmo comienza a ser alto para la red actúa algoritmo de control de congestión Congestion Avoidance (C-A).

- La ventana de congestión CWND es un control impuesto por la fuente, mientras el control de flujo es impuesto por el receptor.

Algoritmo Slow-Start (S-S)

Inicio *conexión: CWND=1 segmento de tamaño máximo (MSS) igual al anunciado por el receptor*

Mientras *CWND<RWND* ***y*** *CWND ≤ SSTHRESH* ***y*** *NoCongestion*

Enviar Nº segmentos=min(CWND,RWND)

*Cuando llega 1 ACK → CWND=2*MSS=CWND+1*

FMientras

Administración Avanzada de Redes TCP/IP

Congestion Avoidance (C-A)

- Una vez que se conoce la capacidad de la red, trata de evitar llegar a la congestión de ésta.

- Congestión: No se recibe el ACK en el tiempo esperado (RTO) o el Nº ACK duplicados = 3

- C-A para que la red se recupere de congestiones sin dejar de transmitir y volver a S-S.

- Durante C-A emisor transmite segmentos de forma lineal para que la red se recupere.

- SSTHRESH=65535 bytes al inicio (umbral de referencia para el valor de CWND).

Congestion Avoidance (C-A)

- Mientras CWND≤SSTHRESH y NoCongestion → S-S

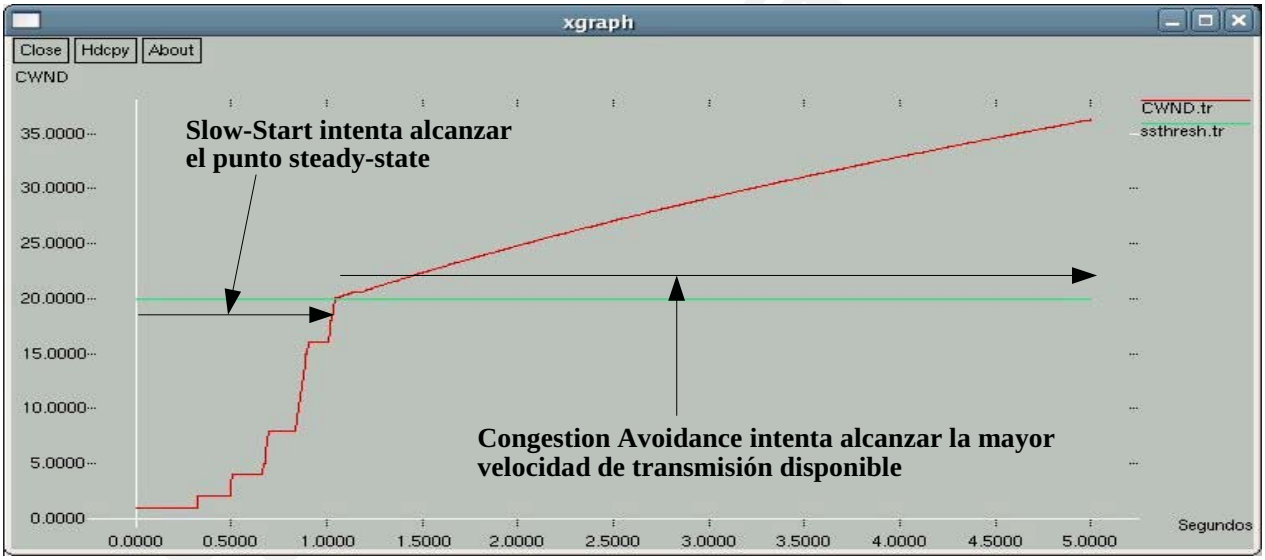
- Si CWND>SSTHRESH o Congestion →C-A

- Si Congestion (RTO o ACK duplicados) →SSTHRES=max(2,Current-Win/2)

  Si RTO → CWND=Initial_Window=1

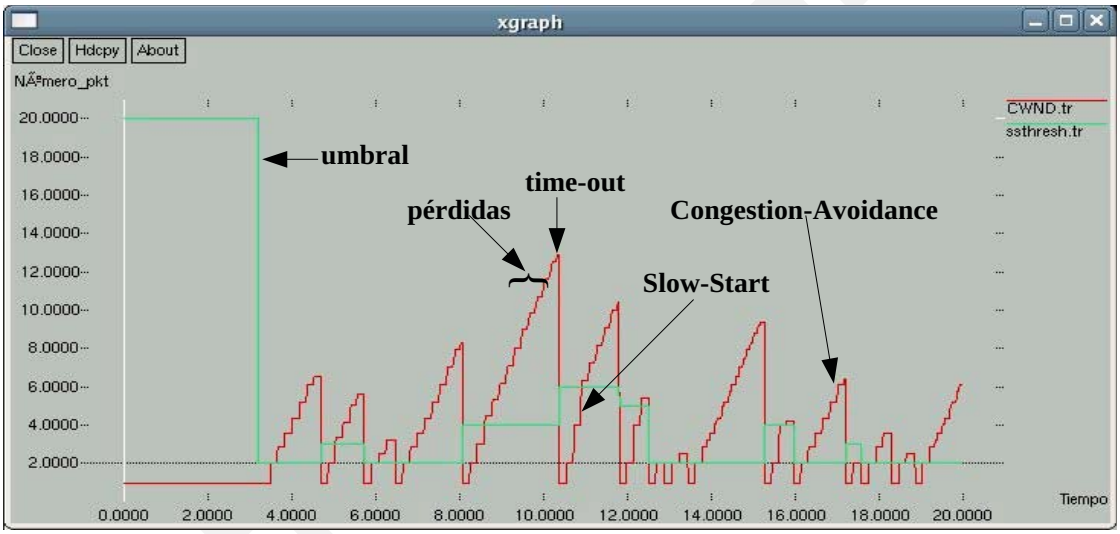
Slow-Start y Congestion Avoidance

- Aunque S-S y C-A se consideren algoritmos diferentes, TCP usa ambos conjuntamente para controlar la congestión en algún punto de la red entre el emisor y el receptor.



Slow-Start y Congestion Avoidance

- Aunque S-S y C-A se consideren algoritmos diferentes, TCP usa ambos conjuntamente para controlar la congestión en algún punto de la red entre el emisor y el receptor.



Control de congestión TCP en dos fases: S-S y C-A

Inicialización:

cwnd = 1 segmento MSS;
ssthresh = valor arbitrariamente grande (*rwnd*, o bien 65.535 bytes);
Rutina de salida de TCP envía siempre el mínimo (*cwnd*, *rmss*) o la *current_window*

Hasta la recepción de un ACK:

Si (*cwnd* ≤ *ssthresh*) /* *Estamos en Slow Start* */
cwnd = *cwnd* + 1(MSS)
Sino /* *Estamos en Congestion Avoidance* */
cwnd = *cwnd* + *1(MSS*MSS)/cwnd*; (*)

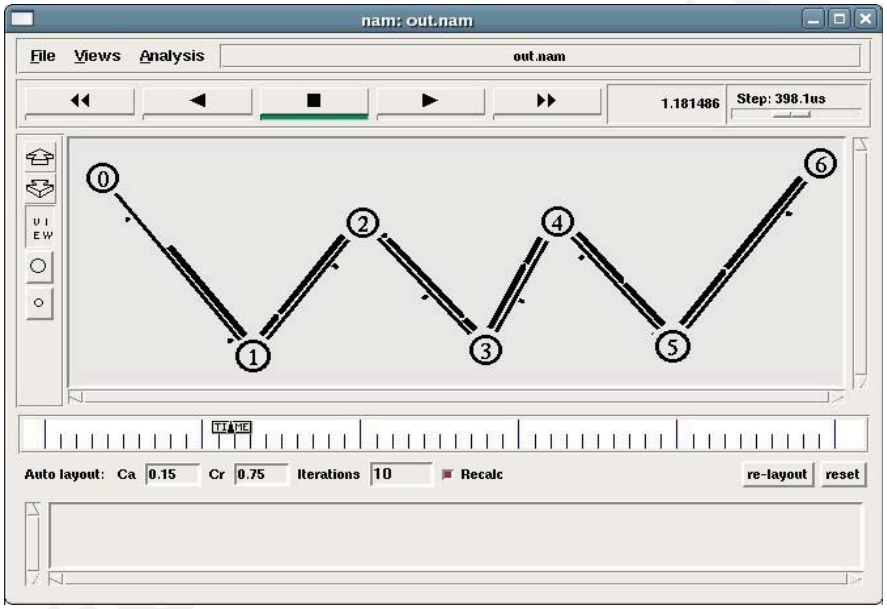
Si Congestión (por timeout o por recepción de 3 ACK duplicados):

Si *timeout* **entonces** *cwnd* = Initial_window=1 y entrada drástica en S-S;
ssthresh = max (2*MSS, *current_window*/2);

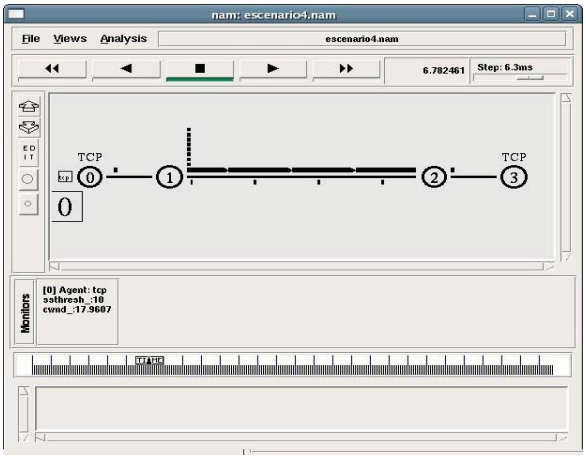
Fin.

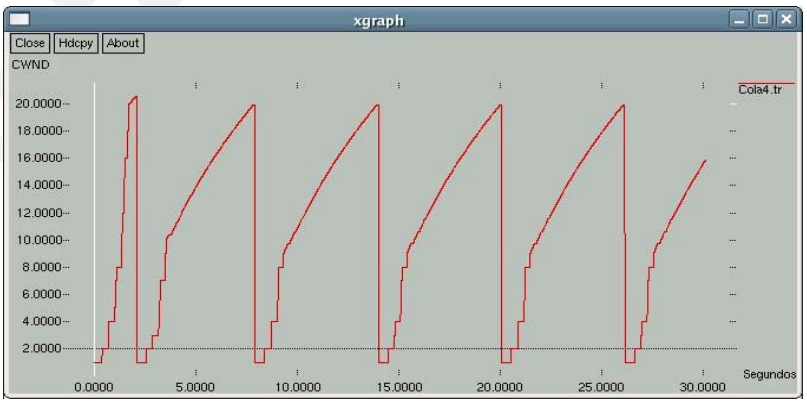
(*) Algunas versiones BSD en C-A hacen
CWND=CWND+(MSS*MSS)/CWND+ MSS/8

4) TCP y sus implementaciones



Administración Avanzada de Redes TCP/IP





Fast Retransmit

lgoritmo de retransmisión rápida (Van Jacobson, 1990) como mejora de TCP.

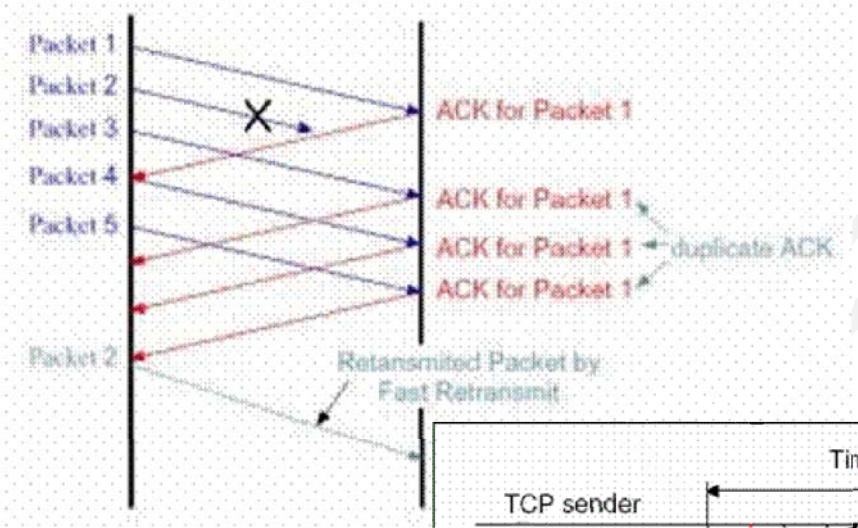
celerar retransmisión de segmentos de datos perdidos en ciertas circunstancias.

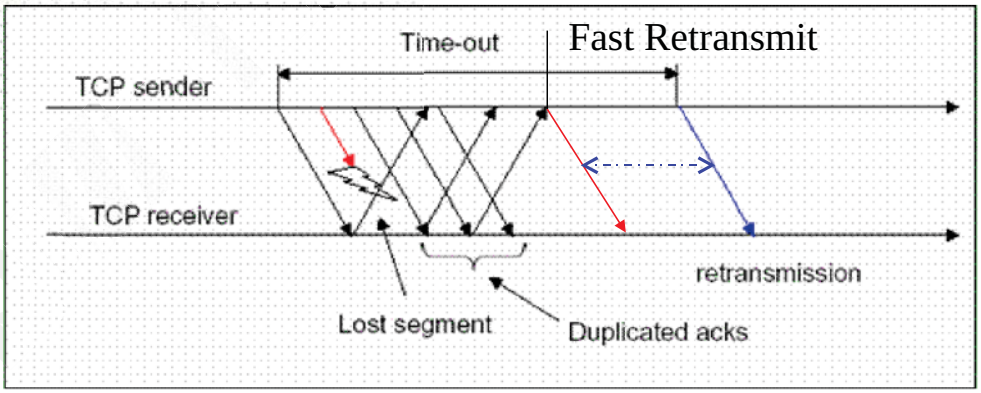
CP puede experimentar pérdidas frecuentes y receptor reciba segmento desordenado
r dos motivos principales:

Pérdida del segmento.

Reordenación de los segmentos en la red por algún motivo y segmento aún pendiente de llegar y lo haga desordenadamente.

ı el primer caso se debe retransmitir el segmento cuya pérdida es asumida por el
nisor cuado recibe el segundo ACK de ese segmento desde el receptor.





Fast Recovery

Interesante en situaciones de congestión pasajeras o puntuales, no interesa bajar CWND al mínimo y volver a S-S.

Mejorar el throughput si se aplica S-S sólo cuando se retransmite por timeout y no por 3 ACK duplicados.

Cuando llega tercer ACK duplicado:

$$ssthresh = \text{máx}\ (current\_window/2,\ 2)$$

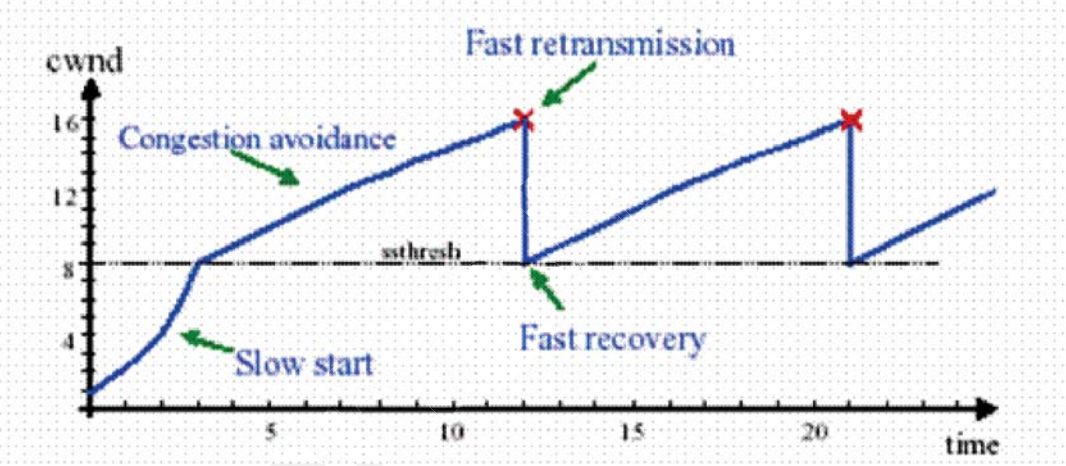
Pero no entra en escena S-S, sino que se retransmite el segmento perdido como en C-A y se establece la ventana de congestión como:

$$cwnd = ssthresh + 3 * (\text{tamaño del segmento})$$

Se hace la retransmisión del segmento perdido en C-A y no en S-S. Se pone ssthresh a la mitad de la cwnd en el momento de detectar la pérdida.

Administración Avanzada de Redes TCP/IP

Fast Recovery



Fast Retransmit y Fast Recovery conjuntamente

Si paquete perdido es detectado por retransmisión de timeout:
Congestión seria.
Poner CWND al valor mínimo y pasar control al algoritmo Slow Start.

Si se reciben 3 ACK duplicados seguidos (4 ACK idénticos sin llegada de ningún otro paquete):
Ajustar *ssthresh*
Retransmitir segmento perdido
CWND=ssthresh + 3* SMSS
(el 3 es por cada uno de los 3 ACK duplicados)

Si se recibe otro ACK duplicado:
CWND=CWND + SMSS
Se transmite un nuevo segmento (si *CWND* lo permite)

Si llega un ACK nuevo:
CWND=ssthresh *(disminuye el valor de la ventana)*
Ejecutar C-A (Este ACK debe reconocer todos los segmentos intermedios enviados entre el segmento perdido y la recepción del tercer ACK duplicado, si ninguno de éstos se ha perdido.
Fin

4) TCP y sus implementaciones

- **TCP de Berkeley** (1983):
  - Versión más antigua y con menos algoritmos.
  - Se basaba en el control de flujo entre emisor y receptor.
  - Todos los problemas se resolvían entre los dos extremos sin considerar lo que ocurre en la red.
  - Objetivo: no ser demasiado compleja.
  - No ofrece buen resultado en redes diferentes, congestionadas o de mala calidad, pues sólo tiene en cuenta el tamaño de la ventana del receptor y no considera el tamaño de la ventana de la red.

4) TCP y sus implementaciones

- **TCP Tahoe** (1988 by Jacobson):
  - Implementado durante el proyecto BSD Unix y precursor de TCP Reno.
  - Usa algoritmos *Slow Start* y *Congestion Avoidance* para detectar estado de la red
  - y el control de flujo para disminuir la pérdida de segmentos.
  - Se incluye *Fast Retransmit* para poder hacer la retransmisión de segmentos perdidos lo más rápidamente posible sin esperar a que expire el *time-out*.
  - Incluye modificación del algoritmo estimador del RTT que establece valores de timeout en las retransmisiones RTO.

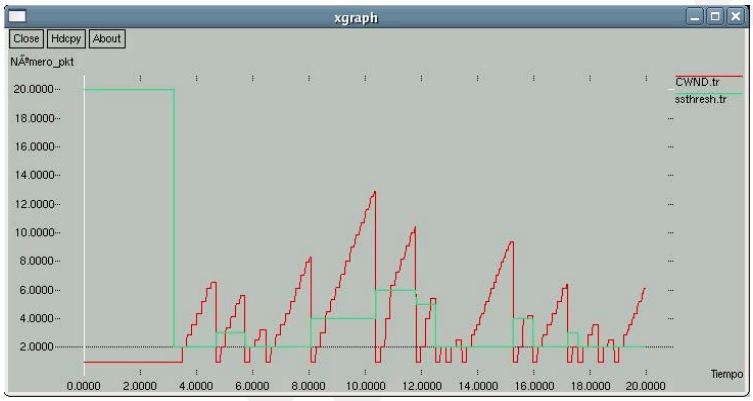
4) TCP y sus implementaciones

- **TCP Reno** (1990): la ventana de congestión crece según *Slow Start* hasta llegar a un umbral previamente definido a partir del cual comienza fase de evitación de congestión creciendo la ventana de forma lineal. Es Tahoe con *Fast Recovery* que evita, en lo posible, que el tamaño de la ventana llegue a dos y se inicie la fase Slow Start en redes que presentan una determinada congestión con picos de gran congestión.

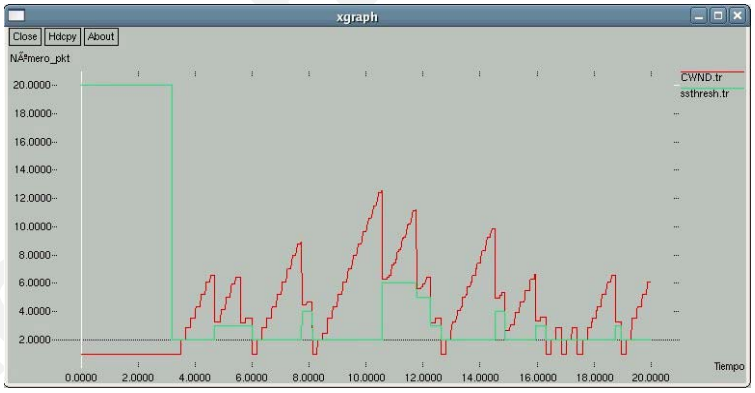
  Cuando expira el timeout:
  CWND=1 y SSTHRESH=CWND/2

  Si se pierden paquetes:
  CWND=SSTHRESH y SSTHRESH=CWND/2
  Al recibir el ACK del segmento retransmitido se restaura
  CWND=SSTHRESH

• **TCP Tahoe:**



• **TCP Reno:**



4) TCP y sus implementaciones

•**TCP Net/3** (1993):

- Añade a Reno soporte multicast y extensiones “long fat network” para superar el límite de 64 K en el tamaño de los segmentos que son un problema en redes con gran retardo o gran ancho de banda (satélite).
- Así se envía pocos segmentos de gran tamaño en vez de muchos de pequeño tamaño.

4) TCP y sus implementaciones

• **TCP New Reno**:

- Intenta solventar los inconvenientes de Slow Start y Congestion Avoidance en relación al tamaño del ssthresh.
- Busca un valor de umbral inicial óptimo para el estado de la red mediante el algoritmo Packet-Pair.
- La fuente envía series de dos paquetes conociendo el intervalo de tiempo entre ambos.
- Según llegan los ACK se va conociendo el retardo y por tanto el estado de la red, la situación de congestión, etc.
- También se usa retransmisión rápida cuando se pierde más de un segmento de una misma ventana.

Administración Avanzada de Redes TCP/IP

4) TCP y sus implementaciones

TCP Sack: (1996-98): Extensión de Reno.

- Para redes con gran probabilidad de pérdidas y/o con tráfico elevado, donde las pérdidas son constantes o excesivas.
- Cuando receptor recibe nuevos datos tras perder un segmento, envía un ACK duplicado a modo de aviso para que el emisor sepa qué segmentos han llegado correctamente y cuáles no, para que sean reenviados.
- Sack realiza constantemente una estimación del tráfico pendiente en la red y sólo envía o retransmite segmentos si el volumen de datos o tráfico estimado es menor que el de la ventana de congestión CWND.
- Usa campo Opciones para enviar un ACK Selective para que el emisor evite retrasos y retransmisiones innecesarias.
- La fuente sólo envía datos (nuevos o retransmitidos) cuando una cantidad de “paquetes excelentes” estimados (llegados al destino ni problemas) es menor que el tamaño de CWND.

4) TCP y sus implementaciones

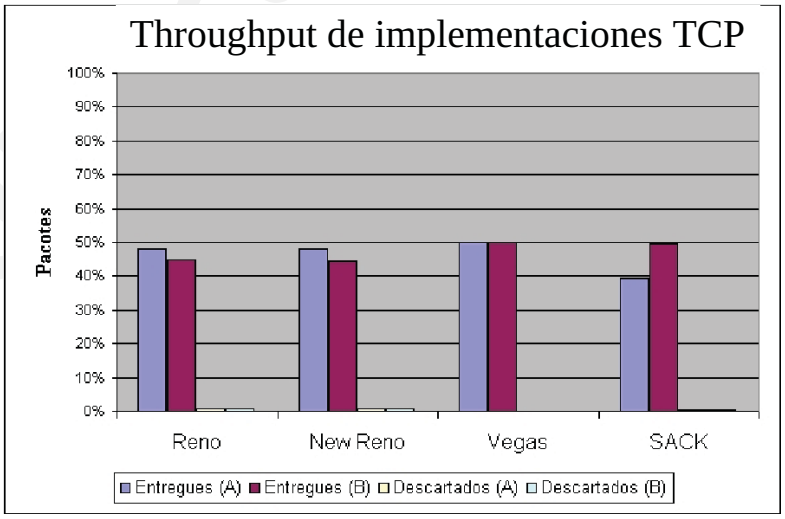
TCP Vegas:

- Aumenta el tamaño de la ventana hasta que ocurre la pérdida del paquete debida a congestión.
- Se fundamenta en el estudio del RTT que se analiza en todos los segmentos.
- Si RTT es grande se asume que la red está congestionada por lo que se disminuye el tamaño de la ventana.
- Si el RTT baja se determina que la red no está congestionada y puede aumentar la ventana.
- Intenta que el emisor detecte de forma anticipada si se puede producir congestión, comprobando constantemente la tasa de transferencia que se espera enviar y la que realmente se logra.
- Intenta mantener un ancho de banda estable y equitativo si hay suficientes buffers en los routers de la red para soportarlo.
- Inmadura.

4) TCP y sus implementaciones

- Dos clientes recibiendo el mismo archivo, para banda de 0,2 Mbps, transmisión de 59,5” y 2.975 paquetes de 500 bytes.

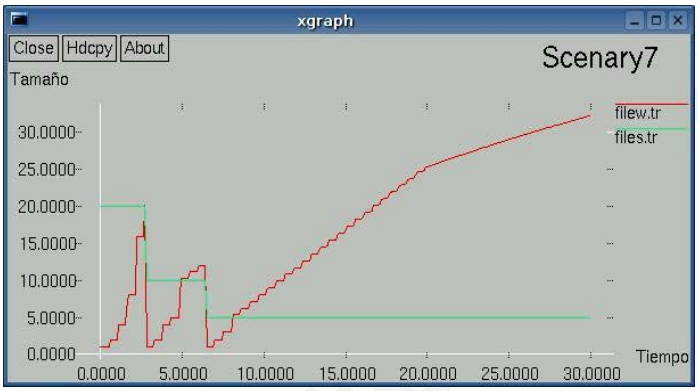
- % paquetes entregados: Vegas 99,9%; Reno 92,8%; New Reno 92,6% y SACK 88,7%



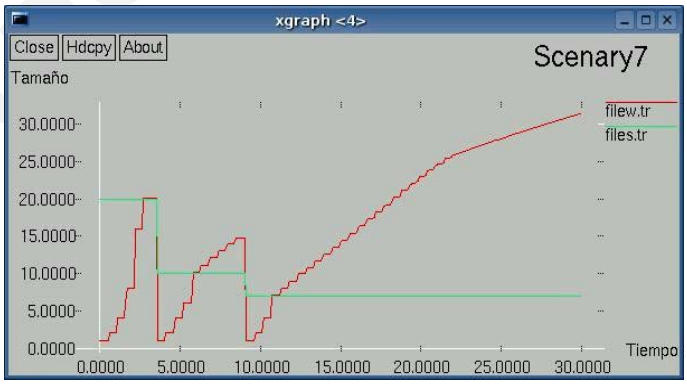
4) Comparación Tahoe y Sack

- Empíricamente se ha demostrado que tamaño de los paquetes típicos en la Red son de: 40, 41, 44, 72, 185, 296, 552, 576 y 1.500 octetos
  Fuente: *http://www.nlanr.net/NA/Learn/packetsizes.html* .

- Enlace de 1.420 bytes, velocidad transferencia de 1 Mbps y 1 paquete/0,05”



TCP Tahoe

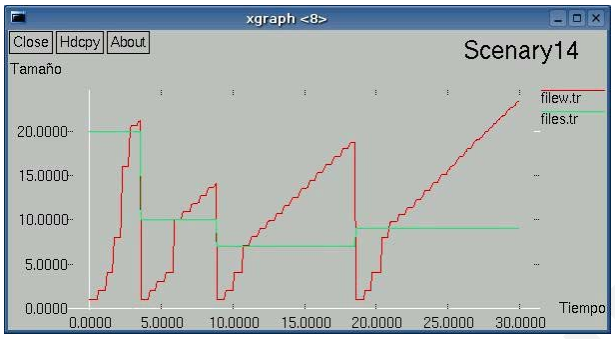


TCP Sack

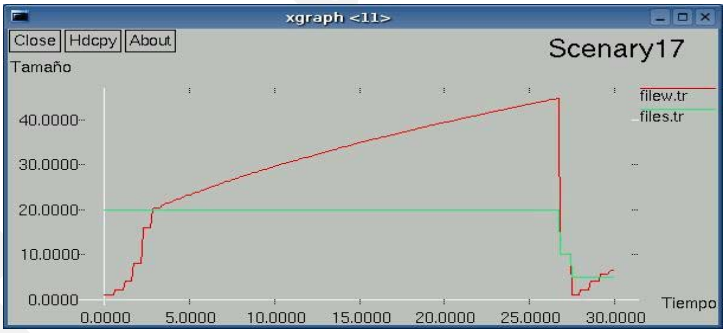
4) Comparación TCP Tahoe, Reno, New Reno y Sack

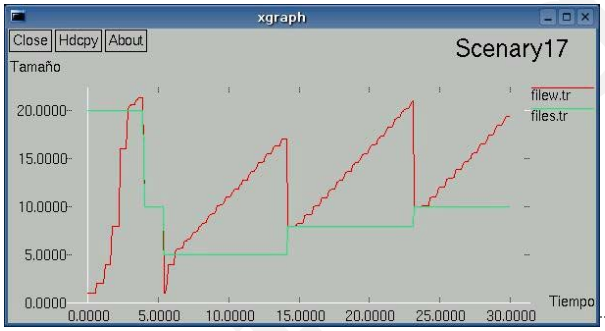
- Paquetes de 1.420 bytes, a 1 paquete/0,005” y 10 Mbps

TCP Tahoe

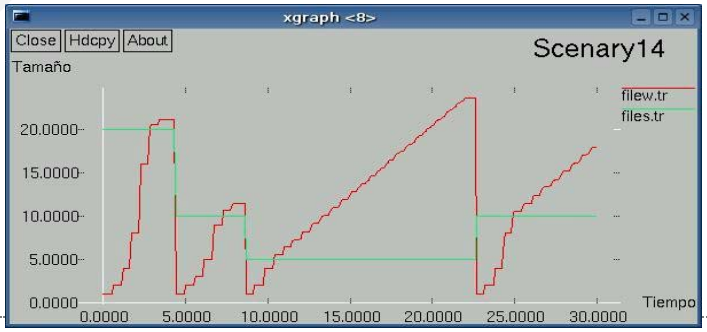


TCP Reno



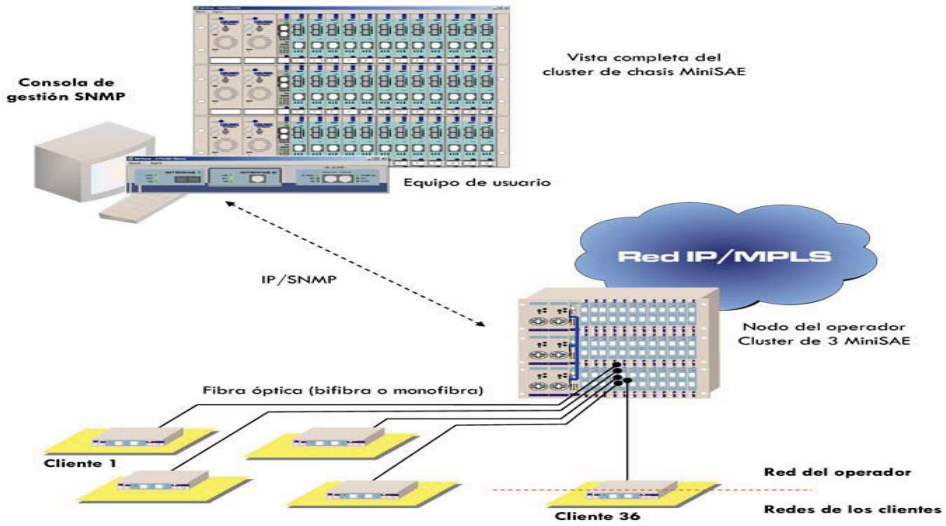


TCP New Reno



TCP Sack

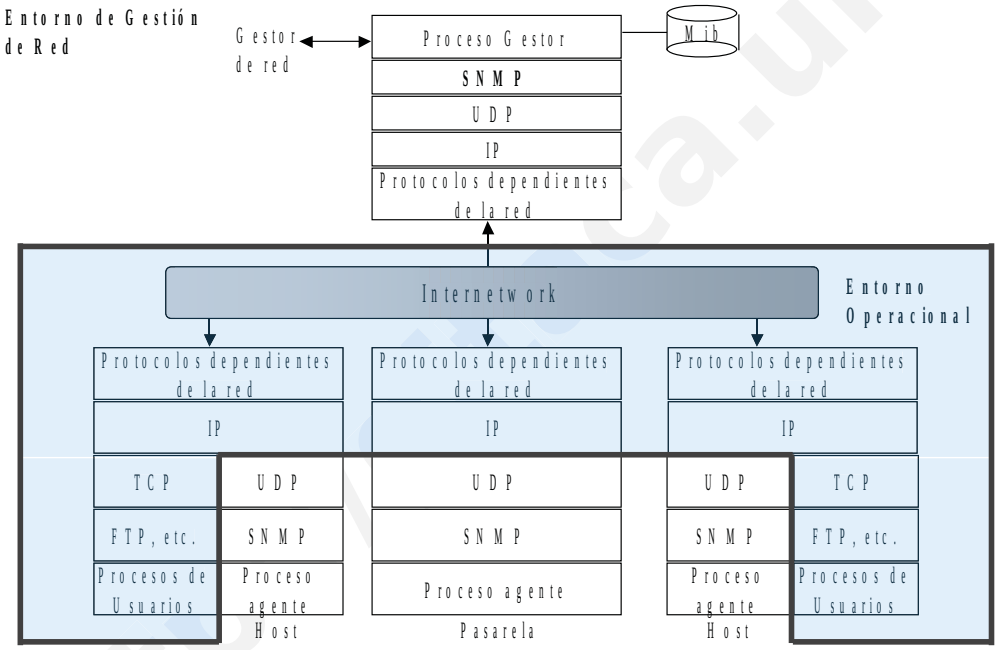
5. Protocolo de gestión de red (SNMP) y de correo (SMTP, POP3 e IMAP4)



SNMP (Simple Network Management Protocol)

- Protocolo encargado de la gestión de los equipos y protocolos que forman Internet.
- Áreas funcionales de la gestión de red, según su ámbito:
  - Fallos: detección y subsanación de problemas en la red mediante la recepción de alarmas, tests y diagnósticos para aislar errores.
  - Contabilidad: análisis del uso de recursos disponibles para evitar la monopolización.
  - Configuración: identificación e interrelación de recursos gestionados y sus características de operación, creacíon de nuevos recursos a gestionar así como su borrado, alertas en tiempo real, obtención de informes a voluntad.
  - Calidad de Funcionamiento: Evaluación del rendimiento de dispositivos y protocolos.
  - Seguridad: soporte a la aplicación de distintas políticas de seguridad de red.
- SNMP es un protocolo de aplicación, por lo que generalmente emplea los mismos protocolos TCP/IP que los protocolos de aplicación de usuario.

Esquema y terminología de la gestión de red



Componentes

- Existen varias especificaciones que definen SNMP, sus funciones y bases de datos afines: RFC 1155 (Estructura e Identificación de la Información de Gestión), RFC 1213 (Base de Gestión de Información MIB-II), RFC 1157 (Simple Network Management Protocol).
- Elementos del sistema de gestión de redes TCP/IP:
  - Estación de Gestión: Es la interfaz entre el gestor de redes (humano) y el sistema de gestión de red. Pregunta a los agentes, pide datos, visualiza alarmas, almacena datos, etc. Debe poseer una base de datos de información extraída de los MIBs de todas las entidades gestionadas en la red.
  - Agente de Gestión: Software que proporciona acceso a los datos de gestión de un elemento de red particular. SNMP proporciona dos clases de transacciones: Petición por parte del gestor SNMP con la respuesta del agente SNMP y Notificaciones no solicitadas (TRAPS) del agente al gestor.
  - Protocolo de Gestión de redes: Permite la comunicación entre la estación de gestión y los agentes. Incluye las capacidades GET, SET y TRAP.
  - MIB (Management Information Base): Conjunto de objetos accesibles en el agente desde el gestor. Una estación de gestión realiza la función de monitorización leyendo el valor de los objetos de la MIB, pero puede también forzar una acción en el agente modificando sus valores.

Sondeo dirigido por TRAP

- El gestor puede sondear periódicamente todos los agentes comprobando si algo necesita atención. Esto es poco práctico si tiene muchos agentes a su cargo.
- La técnica *trap directed polling* consiste en que el gestor sólo se fijará en el agente cuando reciba un *trap* de dicho agente. Pero, como son "no confirmados" y la transmisión puede no ser fiable, el gestor no puede confiar sólo en los traps como aviso de que algo necesita atención, ni tampoco asumir que todo es normal en caso de no recibir ningún trap.
- Lo recomendable es:
  - En la inicialización y a intervalos poco frecuentes, el gestor sondea todos los agentes que conozca solicitando información clave (como características de la interfaz, estadísticas básicas de funcionamiento, etc).
  - Cuando se establezcan estas líneas básicas, la estación de gestión se abstendrá de sondear.
  - En su lugar, cada agente se responsabiliza de avisar a la estación de gestión mediante *traps*, en el caso de que ocurra algún evento de interés.

MIB (Management Information Base)

- La MIB es una base de datos que contiene un conjunto estructurado de los objetos o recursos a gestionar de una red.
- Cada nodo mantendrá una MIB que reflejará el estado de los recursos gestionados de ese nodo. Una entidad de gestión de red puede monitorizar los recursos de dicho nodo leyendo los valores de los objetos en la MIB.
- Para que la MIB pueda servir a las necesidades de un sistema de gestión de red, debe alcanzar dos objetivos:
  - Los objetos utilizados para representar un recurso concreto deben ser los mismos en cada nodo.
  - Cada objeto gestionable SNMP de un dispositivo debe tener un nombre único que se empleará en las operaciones de gestión.
- La versión actual de la MIB para Internet es la MIB-II, que se define en el RFC 123.

SMI (Structure of Management Information)

- La estructura de la información de gestión, especificada en el RFC 1155, define el marco de trabajo general dentro del cual una MIB se puede definir y construir.
- SMI identifica los tipos de datos que se pueden usar en la MIB, cómo se representan y cómo se nombran los recursos dentro de la MIB.
- La filosofía de SMI es favorecer la sencillez y extensibilidad dentro de la MIB. De hecho, ésta sólo puede almacenar tipos de datos simples: escalares y arrays bidimensionales de escalares (tablas). SMI evita las estructuras complejas de datos para simplificar la tarea de la implementación y mejorar la interoperabilidad.
- Para representar la información de gestión de un modo más estándar, SMI debe proporcionar técnicas estandarizadas para:
  - Definir la estructura de una MIB particular.
  - Definir objetos individuales, incluyendo la sintaxis y el valor de cada objeto.
  - Codificar los valores de objetos.

Tipos de datos ASN.1

- *Abstract Syntax Notation 1* es un una notación estándar y flexible que describe estructuras de datos para la representación, codificación, transmisión y decodificación de datos sin ambigüedad. SMI es el subconjunto de ASN1 especificado para definir conjuntos de objetos MIB relacionados.

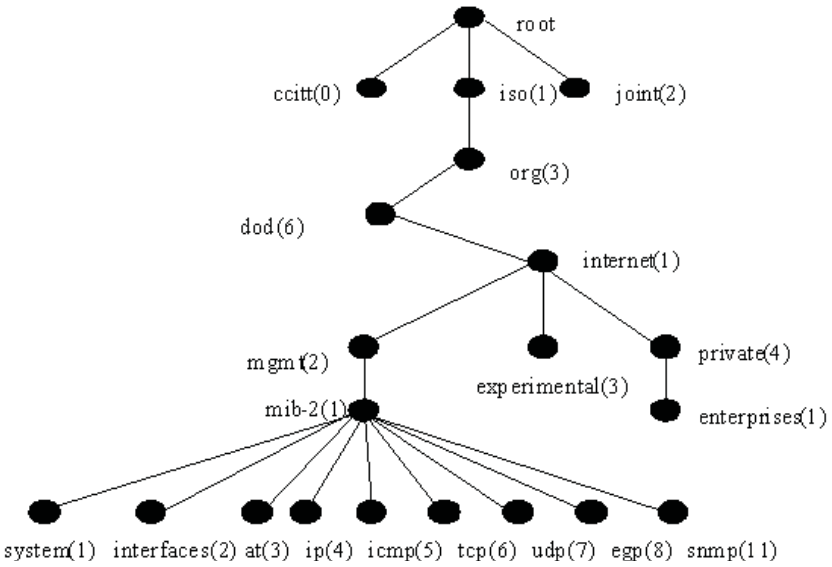
Tipos simples:	INTEGER BITSTRING OCTETSTRING Display String NULL OBJECT IDENTIFIER	**Tipos compuestos:**	SEQUENCE SEQUENCEOF CHOICE

Subtipos:	IpAddress	—	OCTETSTRING de longitud 4 (dirección IP en notación de punto)
	PhyAddress	—	OCTETSTRING de longitud 6 (dirección MAC)
	Counter32	—	contador de 32 bits, ascendente módulo 2^{32}
	Gauge32	—	un entero sin signo en el rango 0 a 2^{32}-1
	Integer32	—	INTEGER de 32 bits
	TimeTicks	—	contador de 32 bits, que se incrementa cada 1/100s

Subconjunto de objetos de la MIB de Internet

```
iso(1)
   org (3)
      dod (6)
      internet (1)
            directory (1)
            mgmt (2)
               mib-2 (1)
                     system(1)
                     interfaces (2)
                     at (3)
                     ip (4)
                     icmp (5)
                     tcp (6)
                        tcpRtoAlgorithm (1)
                        tcpConnTable (13)
                              tcpConnEntry (1)
                                 tcpConnState (1)
                                 tcpConnLocalAddress (2)
                                 tcpConnLocalPort (3)
                                 tcpConnRemAddress(4)
                                 tcpConnRemPort (5)
                     udp (7)
                     egp (8)
                     transmission (10)
                     snmp (11)
                     rmon (16)
            experimental (3)
            private (4)
               enterprises (1)
                     hp (11)
```

iso	org	dod	internet	mgmt	mib-II	tcp	tcpRtoAlgorithm
1	3	6	1	2	1	6	1



Seguridad en SNMP

- El sistema de seguridad de SNMP está basado en el concepto de *community*, que es una relación entre un agente SNMP y un conjunto de gestores, definiendo un control de acceso particular.
- Las estaciones de gestión pertenecientes a una determinada comunidad deberán emplear un *community name* determinado en todas sus operaciones get y set.
- Cuando un agente define una comunidad, está limitando el acceso a su MIB a un cierto conjunto de estaciones de gestión. Además, les puede proporcionar distintas categorías de acceso. Este control de acceso tiene dos vertientes:
  - Vista de la MIB: Es un subconjunto de objetos de la MIB. Se pueden definir diferentes vistas de la MIB para las distintas comunidades.
  - Modo de acceso: Podrá ser *READ-ONLY* o *READ-WRITE*. Para cada comunidad se definirá un método de acceso.
- A la combinación Vista/Modo acceso se le llama *SNMP community profile*. Cuando a cada comunidad se le asocia un perfil de comunidad se habla de la *SNMP access policy*.

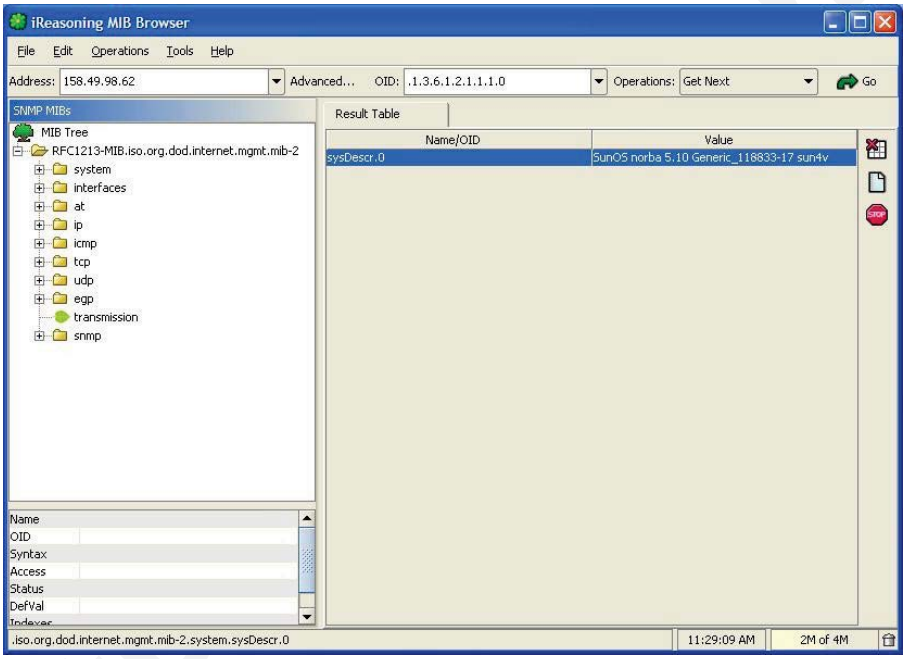
Críticas sobre SNMP

- Madurez: SNMP ha sido probado por la comunidad internet antes de salir como estándar, al contrario de lo que ocurre con ISO. Se ha convertido en un estándar de facto, aceptado por la industria.
- Disponibilidad: Esta soportado por multitud de productos.
- Facilidad de implementación: Es un protocolo sencillo, es fácil de implementar y se ha extendido muy rápidamente. Algunas implementaciones son de dominio público.
- Recursos del sistema reducidos: Al estar basado en datagramas y tener un número reducido de comandos, puede instalarse en dispositivos con capacidad limitada, como bridges, routers, etc. Además, SNMP requiere menos memoria y menos ciclos de reloj que otros protocolos de gestión.
- Falta de seguridad: Cualquier estación puede resetear variables. Las variables MIB definidas como read-only inhabilitan esta orden, pero es una solución parcial. Además, el control de acceso es pobre.
- Mal uso del ancho de banda, debido principalmente a la falta de transferencias en bloque.
- Es un protocolo basado en sondeo (polling).
- Necesita UDP e IP y no soporta otros protocolos.

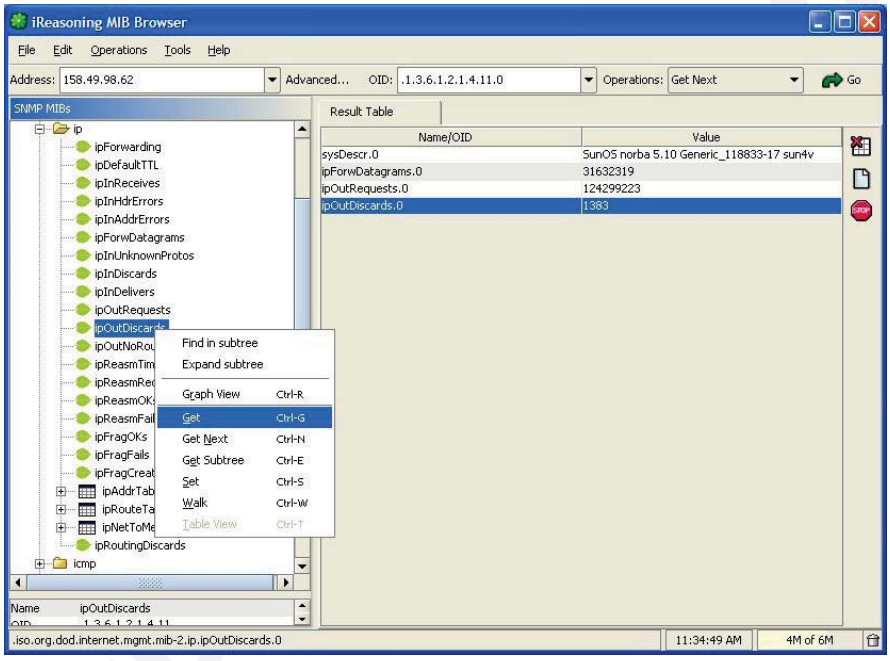
SNMPv2

- La SMI de SNMPv2 expande la Estructura de Información de Gestión (SMI) de SNMP de varias formas:
  - La macro empleada para definir los tipos de objeto se ha ampliado para incluir nuevos tipos de datos y mejorar la documentación asociada a un objeto.
  - Se añade una nueva convención para crear y eliminar filas conceptuales en una tabla.
- La mejora más notable en las operaciones del protocolo es la inclusión de dos nuevas PDUs:
  - *GetBulkRequest* permite al gestor obtener grandes bloques de datos de una manera eficiente.
  - *InformRequest* permite a un gestor enviar información de tipo trap a otro gestor.
- También destacan otras mejoras, como las relativas a seguridad o la capacidad de comunicación *manager-to-manager*.

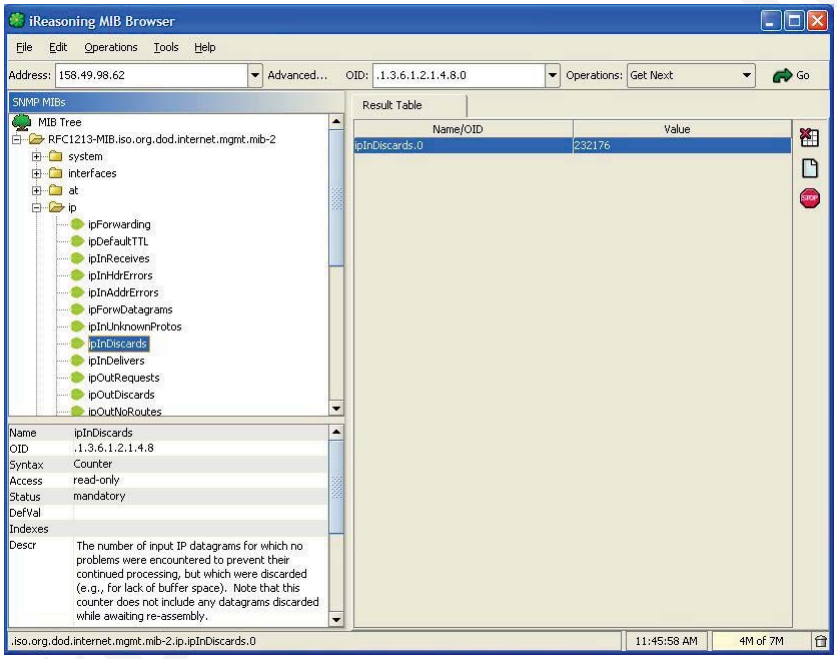
Cliente SNMP: mibbrowser



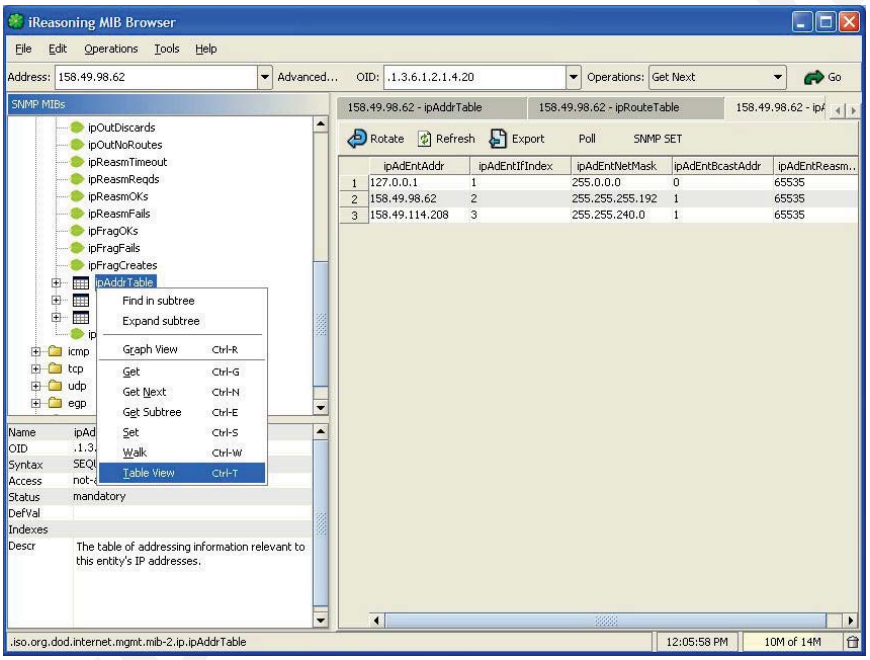
Subárbol IP



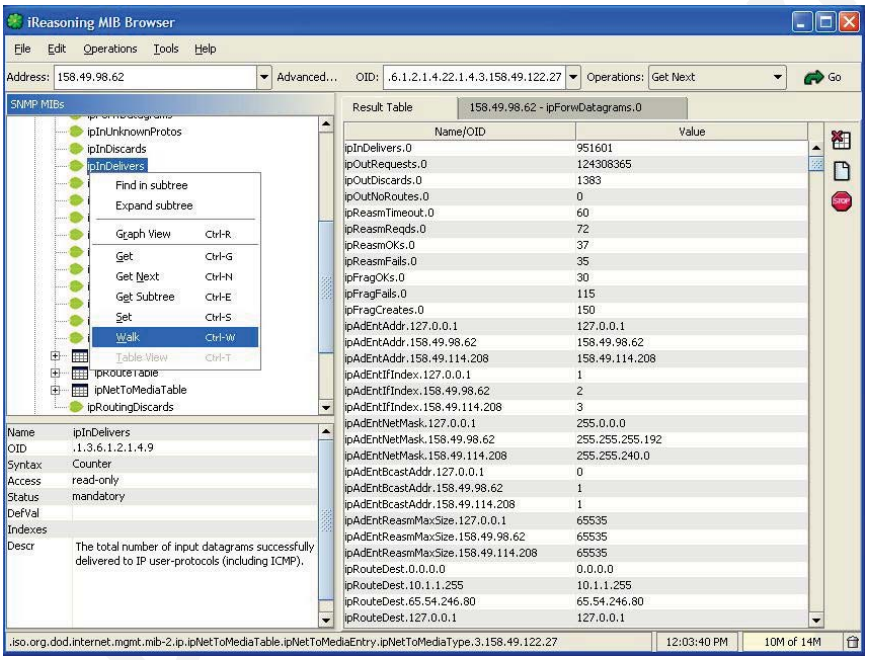
Descripción de objetos



Objetos compuestos

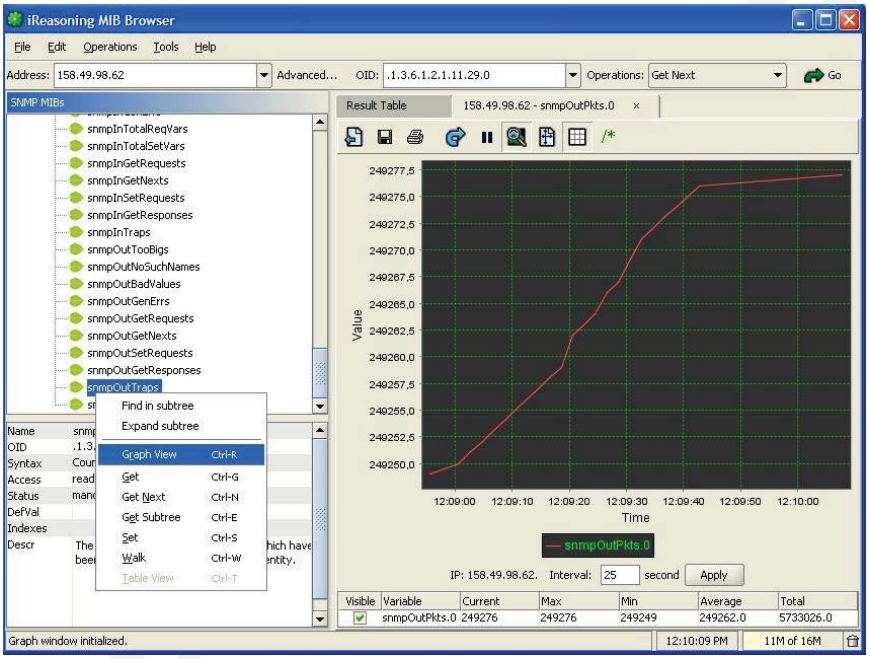


Walking



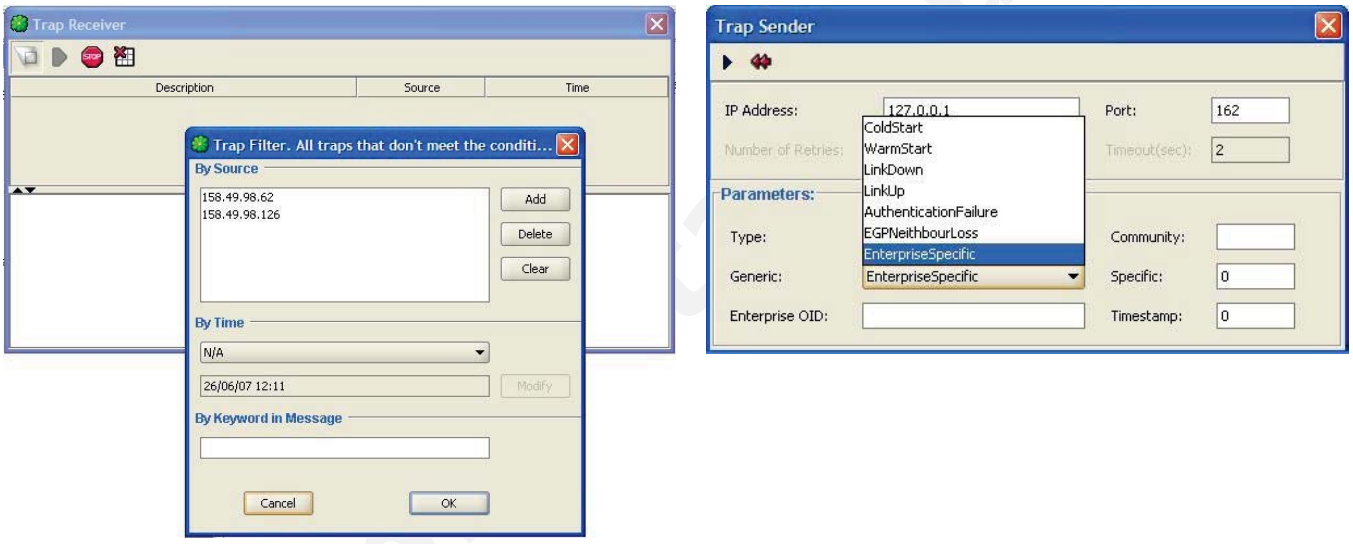
Nº 225

Gráficos de evolución



Nº 226

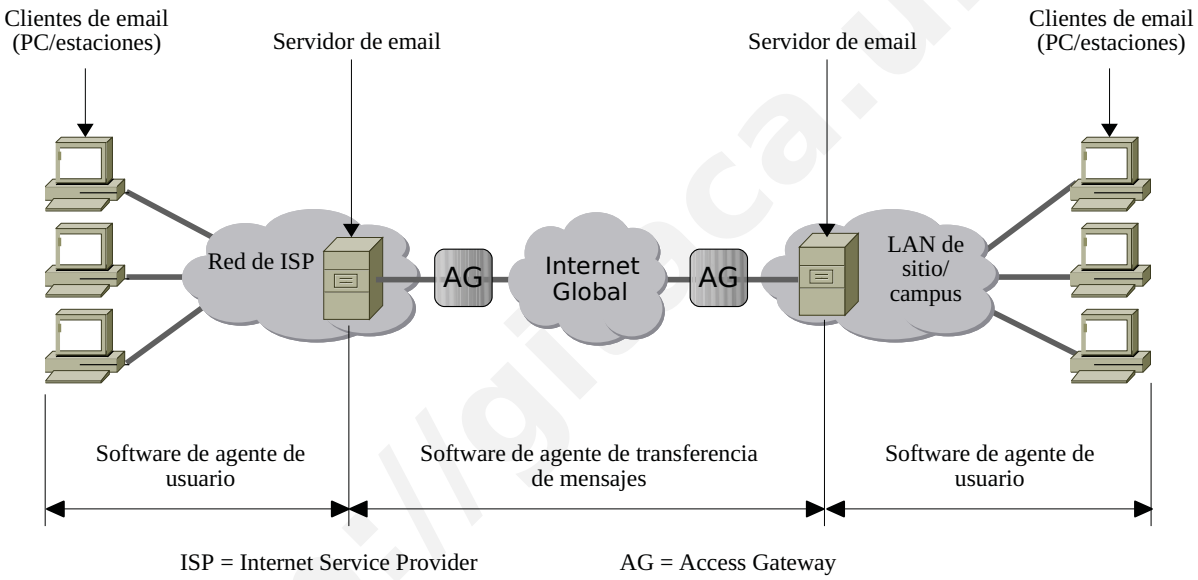
Recepción/envío de traps



SMTP (Simple Mail Transfer Protocol)

- Punto de vista del usuario: correo electronico (e-mail) es el servicio más popular en Internet, aparte de la navegación Web.
- Consta de dos componentes principales:
  - El cliente, que suele ser un PC en el que se ejecuta el UA (*User Agent*) para proporcionar la interfaz de usuario y añadir utilidades para crear, enviar y recibir mensajes. El UA mantiene las bandejas de correo entrante y saliente, así como opciones para manipular mensajes individuales
  - El servidor, que es un computador que mantiene un buzón de correo entrante para cada usuario que mantiene registrado. Posee el UA de servidor que interactuará con el UA de cada cliente, así como un sw para la gestión de la transferencia de mensajes por Internet, el MTA (*Message Transfer Agent*).
- SMTP es el protocolo empleado para el control de la transferencia de mensajes entre dos MTA en Internet. POP3 (*Post Office Protocol 3*) se usa para recoger los correos del buzón de entrada de un usuario y colocarlos en la bandeja de entrada que mantiene el UA.

Correo electrónico en Internet



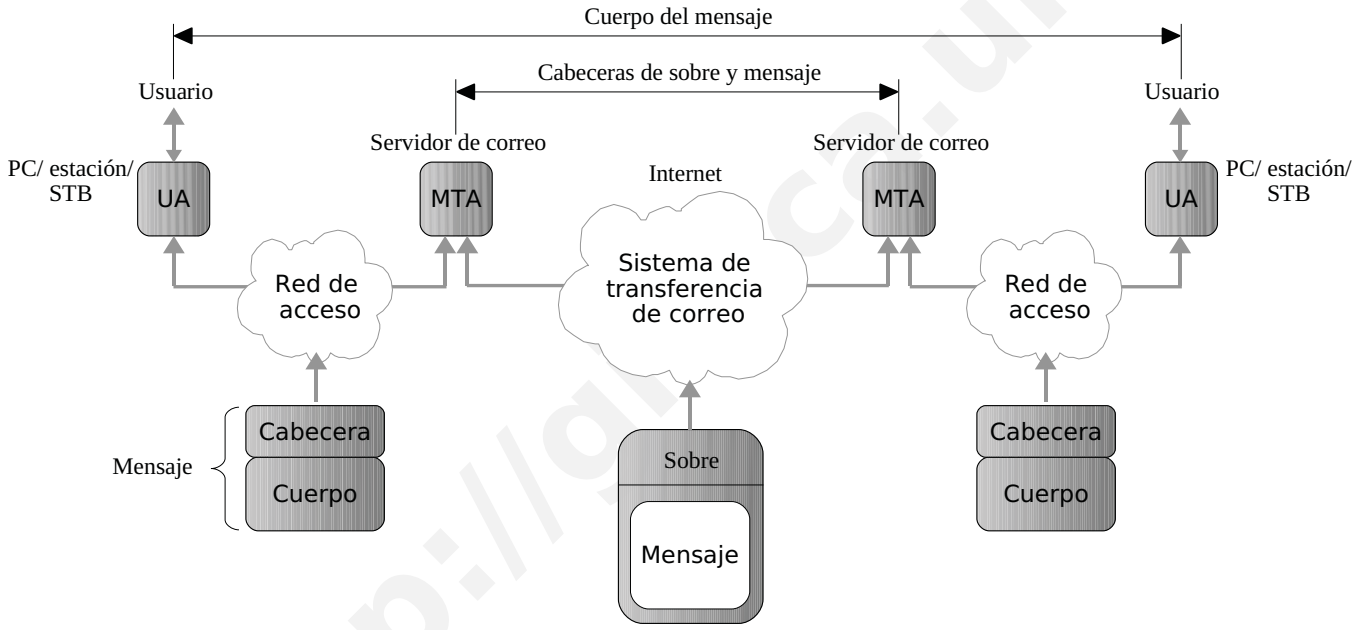
Estructura de mensajes

- De forma similir al sistema de correo postal tradicional, el envío del correo electrónico implica dos procesos: la introducción de diversos campos (remitente, destinatario, etc) y el contenido en sí del mensaje, que puede ser libremente creado por el usuario. Sin embargo la cabecera debe tener una estructura estándar para que pueda ser directamente utilizada por el sistema de transferencia.
- El formato para las direcciones de correo se recoge en el RFC821 y tiene la forma:

  nombre-de-usuario@nombre-de-servidor

- El sistema de transferencia utilizará el *nombre-de-servidor* para encaminar el mensaje por la red y el *nombre-de-usuario* será utilizado por el MTA para determinar en qué buzón de entrada debe depositarlo.
- El mensaje tiene dos partes: cabecera (con varios campos de una lína de texto ASCII cada uno) y cuerpo (creado por el usuario por medio del UA). Se utiliza una línea en blanco para separar ambas partes en el mensaje.

Terminología y uso



Nº 231

Administración Avanzada de Redes TCP/IP

Cabecera de mensaje

Usado también por el sistema de transferencia de correo:

- From: Dirección de correo de la persona que escribió el mensaje
- To: Dirección del destinatario principal
- Cc: Lista de direcciones de otros destinatarios
- Received: Ruta seguida a través del sistema
- Return-Path: Nombre del último MTA

Usado por el usuario/UA:

- Sender: Dirección de correo del que envía el mensaje
- Date: Fecha y hora en que el mensaje fue enviado por el UA
- Message-Id: Identificador único asignado al mensaje por el UA
- Reply-To: Dirección de correo a la que debería dirigirse una posible respuesta
- Subject: Título o asunto del mensaje (una línea)

Definido por el usuario:

- X-PhoneNumber: Número de teléfono del emisor
- X-Fax-Number: Número de fax del emisor
- ...

Nº 232

Contenido del mensaje

- Según el RFC 822, el cuerpo del mensaje sólo puede contener líneas de texto ASCII de hasta 1000 caracteres cada una.
- El estándar se viene usando desde 1983, pero al ampliarse el uso de Internet se incrementó la demanda de otros tipos de mensajes para permitir, por ejemplo que contuvieran datos binarios multimedia, como audio y vídeo.
- Para ello se definió una ampliación al RF822, conocida como MIME (Multipurpose Internet Mail Extensions) en los RFCs 1341, 2045 y 2048.
- Objetivo de MIME: permitir el envío de medios alternativos pero a través del mismo sistema de transferencia. La solución pasa por añadir nuevos campos de cabecera a los ya existentes para especificar el tipo de medio que transportará el mensaje.
- MIME también proporciona el mecanismo para convertir los distintos medios soportados en cadenas de caracteres ASCII que puedan ser transferidas empleando ASCII NVT (Network Virtual Terminal).

Cabeceras MIME

Campos de cabecera adicionales:

Cabecera	Significado
MIME-Version:	Define la versión de MIME que está empleando
Content-Description:	Breve descripción de texto del contenido del mensaje
Content-Id:	Identificador único asignado por el UA
Content-Type:	Define el tipo de información del cuerpo
Content-Transfer-Enconding:	La sintaxis de transferencia empleada
Content-Length:	El número de bytes del cuerpo del mensaje

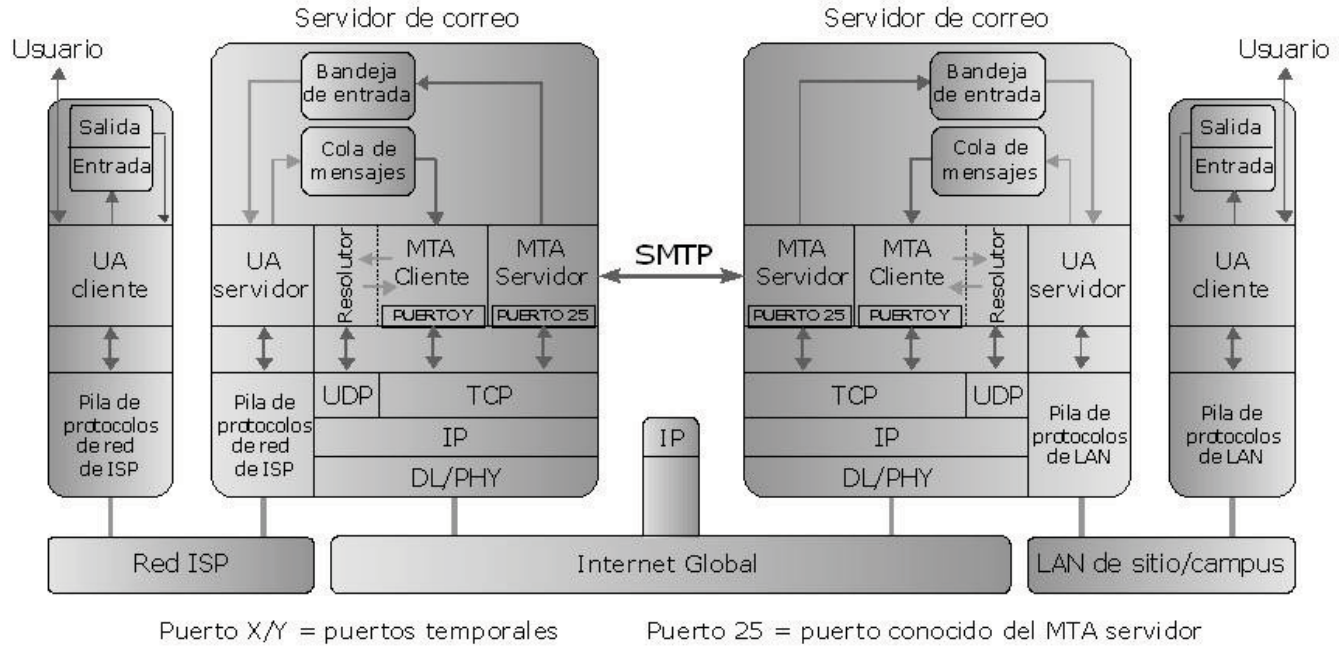
Tipos de contenido alternativos:

Tipo	Subtipos	Descripción
Texto:	Plain:	Texto ASCII sin formato
	Richtext:	Texto formateado basado en HTML
Imagen:	GIF:	Imagen digital en GIF
	JPEG:	Imagen digital en JPEG
Audio:	Basic:	Audio digital
Video:	MPEG:	Secuencia de vídeo o película digital
Application:	Octet-Stream:	Una cadena de bytes
	Postscript:	Documento imprimible en PostScript
Message:	RFC822:	Otro mensaje MIME
	Partial:	Parte de un mensaje más largo
	External-body:	Puntero a donde puede obtenerse el cuerpo de mensaje
Multipart:	Mixed:	Cada parte contiene un contenido o un tipo diferente
	Alternative:	Cada parte con igual contenido y distinto tipo o subtipo
	Parallel:	Las partes deberían mostrarse simultáneamente
	Digest:	Múltiples mensajes

Ejemplo de declaración MIME

```
From: xyz@abc.com
To: abc@xyz.com
Subject: Feliz cumpleaños, Irene
MIME-Version: 1.0
Content-Type: Multipart/Alternative; boundary = “TryAgain”;

--TryAgain

Content-Type: Message/External-body;
 name = “Irene.audio”;
 directory = “Irene”;
 access-type = “anon-ftp”;
 site = “myserver.abc.com”;
Content-Type: Audio/Basic; (Al mensaje de audio se accede de forma remota)
Content-Transfer-Encoding: Base64

--TryAgain

Content-Type: Text/RichText;
<B>***Feliz cumpleaños, Irene***</B> (Mensaje en texto enriquecido)

--TryAgain

Content-Type: Text/Plain;
 ***Feliz cumpleaños, Irene*** (Mensaje en texto plano)

--TryAgain
```


Transferencia del mensaje



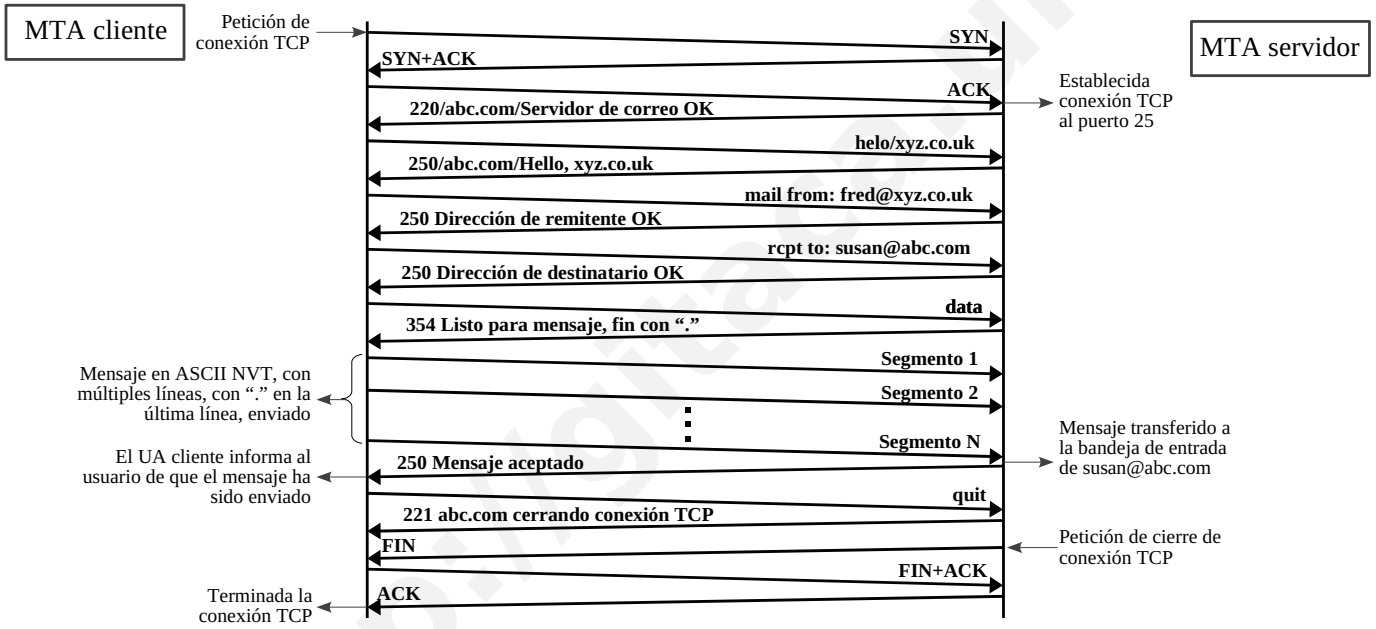
Órdenes SMTP y respuestas

Órdenes (MTA cliente→ MTA servidor)	Descripción
helo <nombre de servidor correo>	Envía el nombre DNS del servidor de correo cliente
mail from: <direccion del remitente>	Dirección del remitente
rcpt to: <dirección del destinatario>	Dirección del destinatario del mensaje
data	Solicitud de envío del cuerpo del mensaje
quit	Solicitud de cierre de la conexión
rset	Cancela la transferencia de correo actual

Resp. (MTA servidor→MTA cliente)	Descripción
220	Servidor destino preparado
221	Servidor destino cerrando conexión TCP
250	Orden cumplida satisfactoriamente
354	El servidor destino está listo para recibir el mensaje
421	Petición de servicio rehusada
450	Buzón no disponible
...	...
551	El usuario no pertenece a este servidor

Respuestas de error

Ejemplo de transferencia SMTP



POP3 (Post Office Protocol 3)

- El protocolo POP3 permite recuperar correo del servidor (ligado usualmente al puerto 110). Define el formato de los mensajes de control intercambiados entre el UA cliente y el servidor, así como la secuencia de mensajes que se intercambian.
- Tipos de comandos POP3:

  - *user*: Lleva como argumento el nombre de usuario.
  - *pass*: Lleva como argumento la contraseña.
  - *list*: Muestra la lista de mensajes pendientes (número y longitud).
  - *stat*: Muestra el número y longitud de mensajes no borrados en el buzón.
  - *top*: Acepta dos argumentos: número de mensaje y número de líneas a recibir.
  - *dele*: Borra el mensaje especificado.
  - *rset*: Recupera los mensajes borrados en la conexión activa.
  - *retr*: Tiene como argumento el número de mensaje que se quiere recuperar completo.
  - *quit*: Abandonar la sesión.

IMAP4 (Internet Messages Access Protocol 4)

- IMAP es un protocol de entrega final alternativo a POP3 definido en el RFC 2060. A diferencia de POP3 que asume básicamente que el usuario vaciará el buzón de cada contacto y trabajará sin conexión después de ello, IMAP supone que todo el correo permanecerá en múltiples buzones de correo en el servidor de manera indefinida.

Característica	**POP3**	**IMAP**
Definición del protocolo	RFC 1939	RFC 2060
Puerto TCP	110	143
Almacenamiento del correo	PC del usuario	Servidor
Lectura de los mensajes	Sin conexión	En línea
Tiempo de conexión requerido	Poco	Mucho
Uso de recursos del servidor	Mínimo	Amplio
Múltiples buzones	No	Sí
Respaldo de buzones	Usuario	ISP
Acceso ubicuo	No	Sí
Control del usuario sobre descargas	Poco	Mucho
Descargas parciales de mensajes	NO	Sí
Problema de espacio en disco	No	Con el tiempo
Facilidad de implementación	Sí	No
Soporte amplio	Sí	En crecimiento

Prueba del servicio SMTP

```
#telnet tajo.unex.es 25
   220 tajo.unex.es ESMTP Exim 3.35 #1 Wed, 06 Jun 2007 12:02:08 +0200
   helo unex.es
   250 tajo.unex.es Hello unex.es [158.49.120.99]
   mail from: usuario@prueba.com
   250 <usuario@prueba.com> is syntactically correct
   rcpt to: usu10@externo.com
   550 relaying to <usu10@externo.com> prohibited by administrator
   rcpt to: compi@alu
   501 compi@alu: malformed address
   rcpt to: compialumnos.unex.es
   501 compialumnos.unex.es: recipient address must contain a domain
   rcpt to: compi@alumnos.unex.es
   250 <compi@alumnos.unex.es> verified
   data
   354 Enter message, ending with "." on a line by itself
   Linea 1 de texto prueba
   Linea 2 de texto prueba
   .
   250 OK id=1HvsO0-0005Nn-00
   quit
   221 tajo.unex.es closing connection

   Se ha perdido la conexión con el host.
```

Administración Avanzada de Redes TCP/IP

Prueba del servicio POP3

```
# telnet tajo.unex.es 110

   +OK POP3 tajo.unex.es v2001.78 server ready [ISafe POP3 Proxy]
   user <usuario>
   +OK User name accepted, password please
   pass <password>  OJO!!
   +OK Mailbox open, 837 messages
   top 3
   -ERR Bad line count argument
   top 3 10
   +OK 2264 octets
   <...10 lineas del mensaje 3...>
   retr 3
   +OK 12862 octets
   <....mensaje 3 completo...>
   quit
   +OK Sayonara.
Se ha perdido la conexion con el host.
#
```

6. Protocolos multimedia

Nº 243

Administración Avanzada de Redes TCP/IP

Antecedentes:

1. Años 70-80:

NVP - Network Voice Protocol

ST – Stream Protocol

2. Años 90:

Mayor parte de los estudios sobre multimedia, Multicasting, Unicast, Tunelling, etc...

3. En estos mementos:

Videoconferencia, televisión digital a través de Internet y recepción de contenidos multimedia

Nº 244

Técnicas de compresión de audio:

- Codificación sub-banda: Este sistema aprovecha ciertas fallas de sistema auditivo humano para codificar una señal a fin de que suene de la misma forma para quien escucha, aunque dicha señal luzca de manera diferente en un osciloscopio. La codificación perceptual se basa en la ciencia de psicoacústica.
- Codificación por transformación de onda: En este tipo de codificación, se transforma de manera matemática en sus componentes de frecuencia mediante una transformación de Fourier. Por tanto la amplitud de cada componente se codifica en una forma mínima. El objetivo es reproducir la forma de onda de manera precisa en el otro extremo utilizando los menos bits posibles.

Técnicas de compresión de vídeo (I):

- Todos los sistemas de compresión requieren dos algoritmos: uno para la compresión delos datos en el origen y otro para la descompresión en el destino.
- Estos algoritmos tienen ciertas asimetrías. Primero, en muchas aplicaciones, sólo se codificará una vez (cuando se almacena en el servidor multimedia), pero se decodificará miles de veces (cuando los clientes lo vean). Esta asimetría significa que es aceptable que el algoritmo de codificación sea lento y requiera hardware costoso, siempre y cuando el algoritmo de decodificación sea rápido y no requiera hardware costoso. Muchos sistemas de compresión prácticos llegan a extremos considerables para lograr que la decodificación sea rápida y sencilla, aun al precio de hacer lenta y complicada la codificación.

Técnicas de compresión de vídeo (y II):

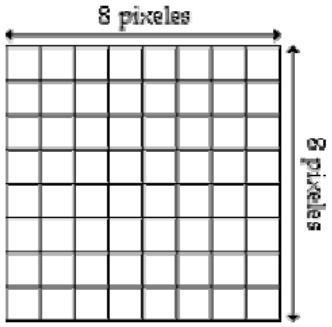
- Por otra parte, para la multimedia en tiempo real, como las videoconferencias, la codificación lenta es inaceptable. La codificación debe ocurrir al momento, en tiempo real. En consecuencia, la multimedia en tiempo real usa algoritmos o parámetros diferentes que el almacenamiento de vídeos en disco, lo que con frecuencia resulta en una compresión significativamente menor.
- Una segunda asimetría es que no es necesaria la capacidad de invertir el proceso de codificación/decodificación. Es decir, al comprimir, transmitir y descomprimir un archivo de datos, el usuario espera recibir el original, correcto hasta el último bit. En multimedia este requisito no existe. Por lo general, es aceptable que la señal de vídeo después de codificar y decodificar sea ligeramente diferente a la original. Cuando la salida decodificada no es exactamente igual a la entrada original, se dice que el sistema es con pérdida (loosy). Si la entrada y la salida son idénticas, el sistema es sin pérdida (lossless). Estos sistemas con pérdida son importantes porque aceptar una pequeña pérdida de información puede ofrecer ventajas enormes en términos de la posible relación de compresión.

Técnicas de compresión de vídeo: Componentes

- 1. Digitalización, muestreo y segmentación – Transformación de señales analógicas en señales digitales.
- 2. Reducción de redundancia – Transformación de datos correlativos (Imágen sin pérdida).
- 3. Reducción de la entropía – Descarte de algunos bits
- menos significativos (Imágen con pérdida)
- 4. Codificación de entropía – Asignación de cadenas de bits de tamaño más pequeño que las cadenas originales.

Codificación de vídeo (I)

- Cálculo de la DCT: Se divide la imagen en bloques de píxeles de tamaño 8x8, que se procesan de izquierda a derecha y de arriba abajo. Según se va encontrando cada bloque o subimagen de 8x8, se cambian los niveles de sus 64 píxeles, sustrayendo de los mismos la cantidad 2n-1, siendo 2n, el máximo número de niveles de gris. Esto es, para las imágenes de 8 bits se resta 128 de cada píxel. Después se calcula la Transformada Discreta del Coseno bidimensional del bloque, produciendo un conjunto de 64 valores conocidos como coeficientes de DCT.



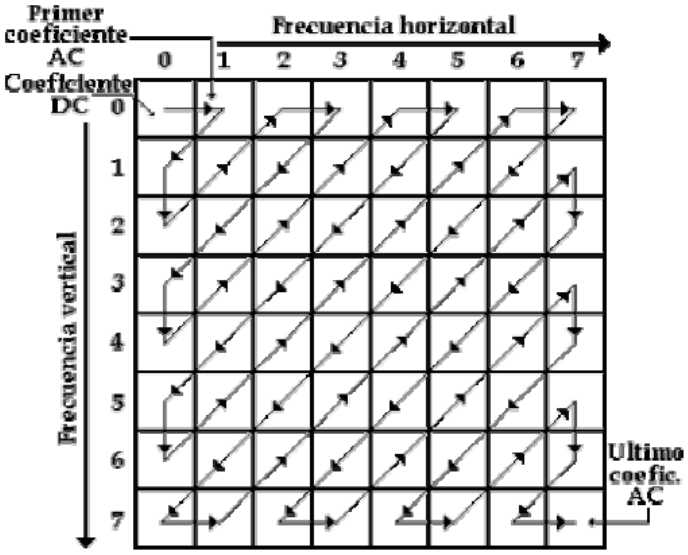
Nº 249

Codificación de vídeo (II)

- Cuantificación de los coeficientes de la DCT: Los 64 coeficientes son entonces cuantificados, produciendo en algunos de ellos su reducción a cero. Los coeficientes son codificados en umbral, usando una matriz de cuantificación y son preparados para la codificación de entropía convirtiéndolos en una cadena unidimensional de 64 coeficientes en orden cuasi ascendente de los componentes de frecuencia. Para convertir los coeficientes en esta cadena unidimensional se reordenan usando una exploración o barrido en zig-zag. El primer coeficiente del barrido en zig-zag es conocido como el coeficiente DC mientras que el resto son los coeficientes AC. A la matriz de cuantificación se le pueden aplicar factores de escala para obtener diversos niveles de compresión. Las entradas de la matriz de cuantificación son usualmente determinadas según consideraciones psicovisuales, las cuales son discutidas más adelante.

Nº 250

Codificación de vídeo (III)

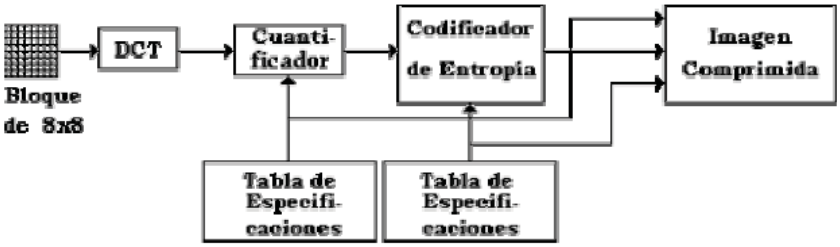


Nº 251

Administración Avanzada de Redes TCP/IP

Codificación de Vídeo (y IV)

- Asignación del Código de Longitud Variable (VLC): El coeficiente DC de cada bloque es codificado usando DPCM. Es decir, se codifica la diferencia entre coeficiente DC del presente bloque y el del bloque previamente codificado. Puesto que la cadena unidimensional reordenada según el barrido en zig-zag de la está distribuida cualitativamente según una frecuencia espacial creciente, el procedimiento de codificación JPEG ha sido diseñado de modo que se beneficia de la existencia de largas series de ceros que se producen normalmente en la reordenación. En particular, los coeficientes AC no nulos se codifican utilizando un código de longitud variable que define el valor del coeficiente y el número de ceros precedentes. Se proporcionan unas tablas de especificación estándar de códigos de longitud variable.

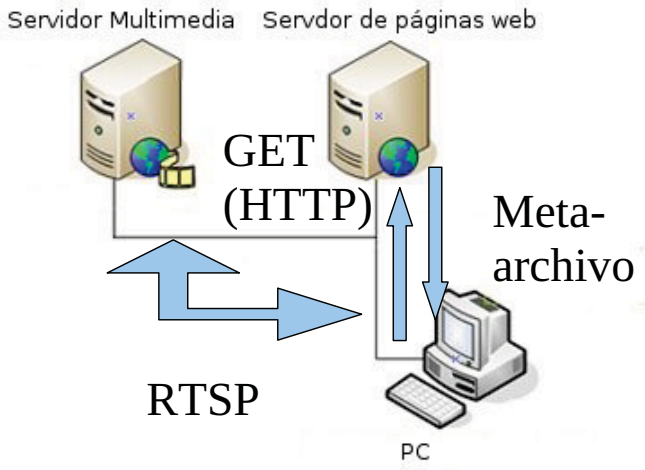


Nº 252

Tipos de transmisiones:

- Flujo Contínuo (Streaming)
- Unidifusión TCP
- Multicast

Multimedia Bajo Demanda (Flujo Contínuo) (I)

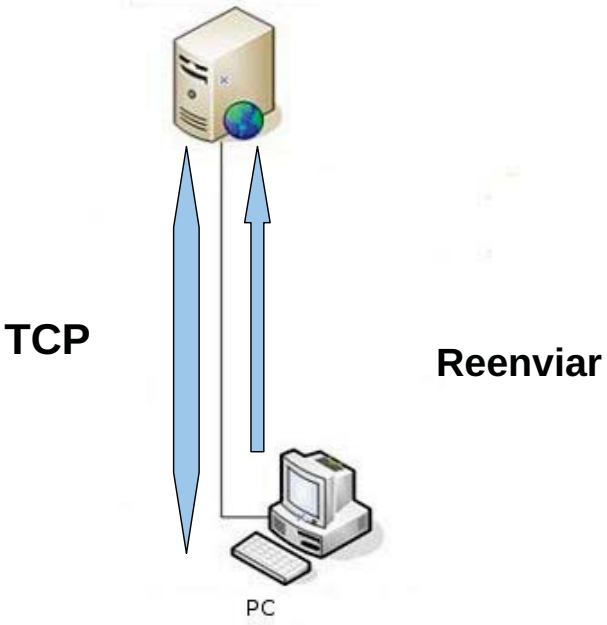


Multimedia Bajo Demanda (Flujo Contínuo) (y II)

- El proceso del multimedia bajo demanda es simple, se inicia cuando un usuario al usar alguna aplicación que sirva este tipo de multimedia pida al programa un archivo de audio, en este momento el navegador es el programa que se activa, estableciendo una conexión TCP con el servidor Web con el que el audio está vinculado. El siguiente paso es el de enviar una solicitud GET en HTTP para pedir el archivo, el servidor al recibir la petición busca en su disco duro el audio almacenado lo devuelve al servidor Web y este a su vez al servidor Web del cliente.
- El navegador cliente investiga, mediante el tipo MIME o por extensión del archivo, cómo se supone que debe desplegar el archivo.
- La forma usual que tienen los navegadores para comunicarse con una aplicación auxiliar (encargada del despliegue) es escribir el contenido en un archivo de trabajo, donde guardará en el disco el archivo multimedia y finalmente el reproductor comenzará la reproducción del mismo.

2. Streaming (I):

- Flujo TCP

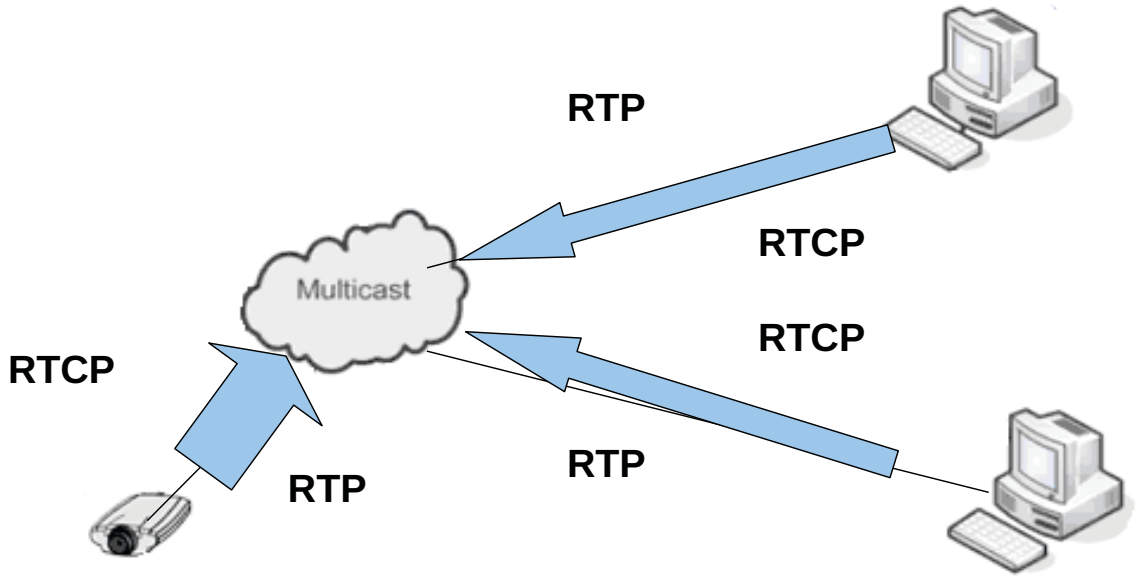


Streaming (y II)

- Es el método usado para difundir el contenido en vivo a traes de Internet. Algunas de las técnicas que se aplican a la multimedia bajo demanda también se aplican a streaming, pero también hay algunas diferencias clave.
- Un punto en el que coinciden es la necesidad de almacenar en el búfer del usuario para disminuir la fluctuación. Al recolectar 10 o 15 segundos de contenido antes de comenzar la reproducción, este se puede percibir sin muchos problemas, aunque suceda fluctuación sustancial a través de la red. En tanto todos los paquetes lleguen antes de que se necesiten, no importa cuándo lleguen.
- Una diferencia clave es que la multimedia bajo demanda puede enviarse a una tasa mayor que la de reproducción, puesto que el receptor pude detener la comunicación. Esto le da el tiempo necesario para retransmitir los paquetes perdidos. En contraste el streaming es que siempre se difunde a la tasa exacta a la que se genera y a la que se reproduce. Otra diferencia es que el streaming por lo general tiene cientos o miles de escuchas simultáneos mientras que la multimedia bajo demanda es de punto a punto.

Multicast (I):

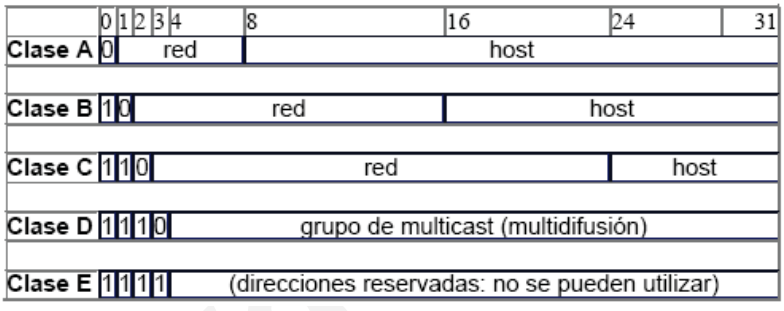
- Grupo de usuarios que reciben todos la misma información



Multicast (II)

- Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes. Los restantes 24 bits se emplean para el número de host, de modo que cada red tener hasta 16,777,214 hosts.
- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16382 redes de hasta 65534 hosts cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2,097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
- Las direcciones de clase E se reservan para usos en el futuro

Multicast (III)



- Por lo tanto, el rango de direcciones de grupos de multicast va del 224.0.0.0 a 239.255.255.255. Para cada dirección multicast hay un conjunto de cero o más hosts a la escucha. Es lo que se denomina el grupo de hosts. Para que un host envíe un mensaje a ese grupo no se requiere que pertenezca a él.

Multicast (y IV)

- Hay dos clases de grupos de hosts:
  - Permanentes: La dirección IP tiene una asignación permanente a través de IANA.
  - Provisionales: Cualquier grupo que no sea permanente es provisional y está disponible para ser asignado dinámicamente según las necesidades. Los grupos provisionales d ejan de existir cuando el número de sus miembros se hace cero.

Tablas comparativas para transmisión de vídeo

Estándar	*Velocidad (Mbps)*
JPEG	0,25-8
MPEG-1	1-1,5
H.261	0,064-2
MPEG-2	4-6
HDVT	17

	MPEG1	MPEG2	MPEG4
Tamaño típico de imagen	352x240(perfil estándar)	720x480(perfil principal @máximo nivel)	720x480 (perfil principal, L2)
Ancho de banda típico	1.5Mbps	5Mbps	2Mbps
Ancho de banda máximo	2.5Mbps	15Mbps	4Mbps

Tabla comparativa de transmisión de audio

Estándar	Velocidad (Kbps)
G.721	32
G.728	16
G.722	48-64
MPEG-2	320

Calidad	Aplicación	Tolerancia de retardo (mseg)	Tolerancia de jitter (mseg)
Baja	Videoconferencia a 64 Kbps	300	130
	Audio a 16 Kbps	30	130
Alta	Vídeo MPEG NTSC a 1,5 Mbps	5	6,5
	Audio MPEG a 256 Kbps	7	9,1
Muy Alta	Vídeo HDVT a 20 Mbps	0,8	1

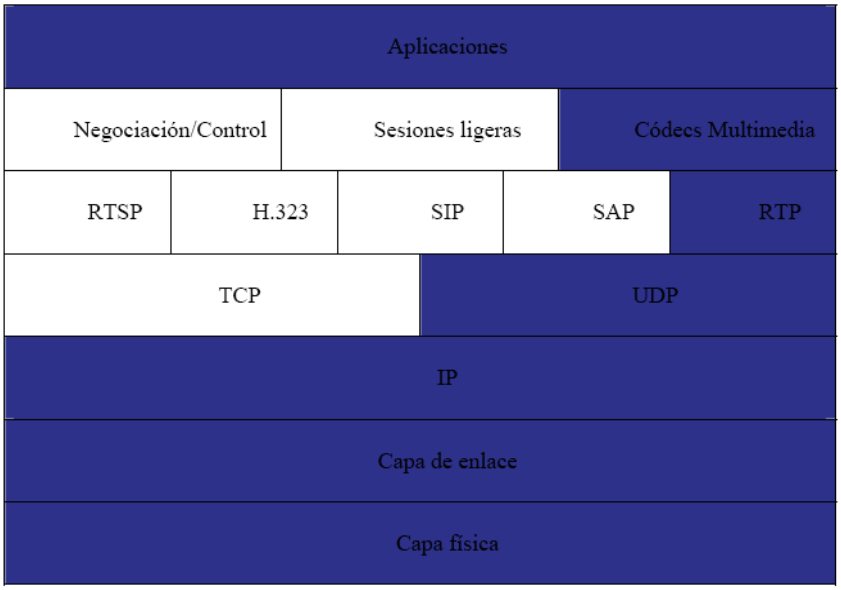
RTP/RTCP (I)

- RTP provee una base para el transporte de medios de comunicación de tiempo real. El perfil de RTP para audio y videoconferencias con el control mínimo estaba normalizado al mismo tiempo que se propuso RTP. Cada perfil es acompañado por algunas especificaciones de payload, cada una de los cuales describen el transporte de un formato multimedia.
- RTP fue publicado por la IETF (RFC 1889) en enero de 1996 y su revisión para el draft está casi completa.
- RTP se asienta sobre el nivel UDP / IP, aumentando las primitivas de este nivel. La mayoría de las implementaciones de RTP son partes de una aplicación o biblioteca que se apoyan en los socket UDP / IP que son provistos por el sistema operativo. Este no es el único diseño posible, ya que el protocolo de RTP no requiere de UDP o IP. Por ejemplo, algunas implementaciones separan en capas RTP encima de TCP/IP, y los otros usan RTP en redes no- IP, como redes ATM.

RTP/RTCP (II)

- RTP se puede dividir en dos partes: el protocolo de transferencia de datos y el protocolo de control asociado.
- El protocolo de transferencia de datos de RTP dirige la entrega de los datos de tiempo real, como audio y vídeo, entre sistemas finales. Define un nivel de descripción de payload de los medios de comunicación, un número de secuencia para la detección de pérdida, tiempo de reproducción para permitir la recuperación de cronometraje, payload, y un indicador para los eventos importantes dentro del flujo de datos.
- El protocolo de control de RTP (RTCP) suministra la realimentación de calidad de recepción, la identificación de participantes, y la sincronización entre flujos. RTCP dirige a RTP y provee de esa información de forma periódica. Aunque los paquetes de datos son enviados normalmente cada milésimas de segundo, el protocolo de control opera en una escala de segundos. La información enviada en RTCP es necesaria para la sincronización entre flujos de datos, por ejemplo, para la sincronización entre el audio y el video y puede ser útil para adaptar la transmisión de acuerdo con la realimentación de calidad de recepción, y para identificar a los participantes.

RTP/RTCP (III)

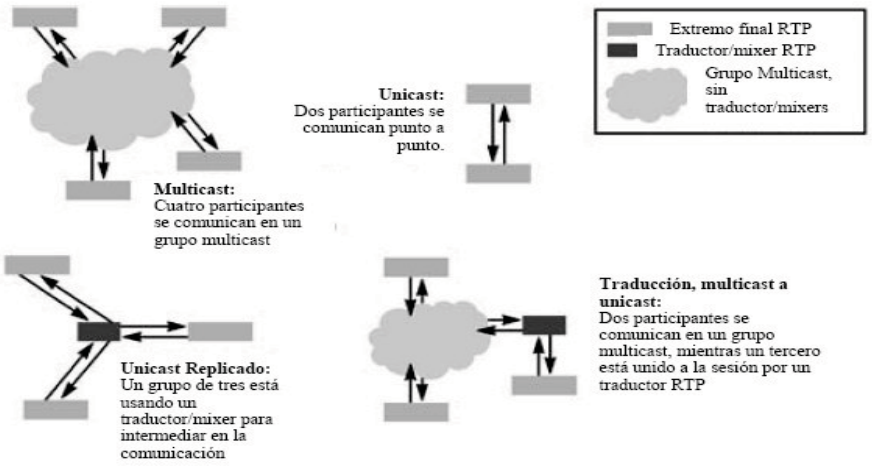


RTP/RTCP (IV)

- Varios protocolos de configuración de llamada, de control y de anuncio pueden ser usados al comenzar una sesión de RTP, dependiendo del escenario donde nos movamos:
  - Para el propósito de empezar una sesión interactiva, ser él una llamada de telefonía de voz o una videoconferencia, existen dos Standard. El Standard más usado en este área era H.323 de recomendación de ITU, y más recientemente la IETF han definido el protocolo de iniciación de sesión (SIP).
  - Para el propósito de empezar una sesión de no interactivas por ejemplo, el video sobre demanda, el Standard principal es el protocolo de transmisión continua de tiempo real (RTSP).
  - El uso original de RTP era con multicast de IP y el modelo de sesiones ligero de conferencia. Este diseño usa el protocolo de anuncio de sesión (SAP) e IP para anunciar las sesiones en curso, como seminarios y transmisiones de la TV, que estaban abierto al público.

RTP/RTCP (y V)

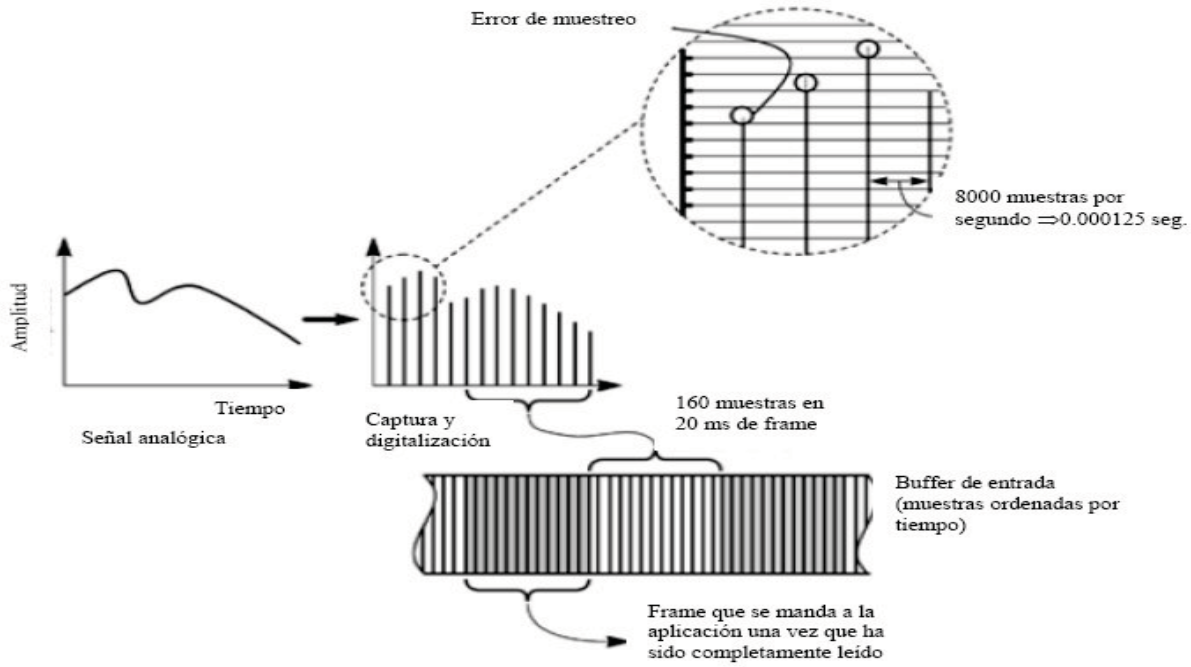
- Los modos de uso de RTP:



Fases de una comunicación multimedia:

- 1. Captura multimedia y compresión
- 2. Generación de paquetes RTP
- 3. Recepción de paquetes
- 4. Decodificación, Mezclado y Reproducció

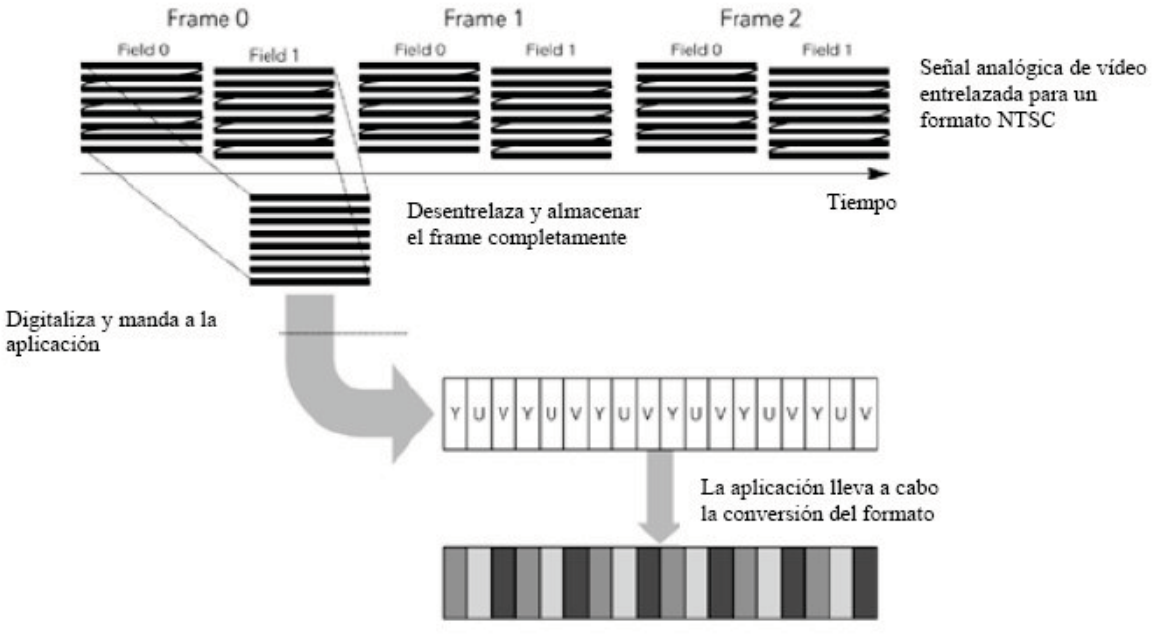
Captura multimedia y compensación: Audio



Captura del audio

- El audio sin comprimir es devuelto por el dispositivo de captura con un tipo de muestreo y con un rango de frecuencias específico. Los dispositivos de captura de audio comunes pueden devolver muestras con 8, 16 o 24 bits, usando cuantización lineal, μ - law o A – law, con frecuencias entre 8,000 y 96,000 muestras por segundo, en mono o stereo. Dependiendo de la capacidad del dispositivo de captura y del códec podría ser necesario convertir el flujo multimedia en otro formato antes de que pueda ser usado.
- Las tramas de audio una vez capturados son pasadas al codificador para la compresión. Dependiendo del códec, los parámetros de compresión pueden ser mantenidos por el códec o pueden ser con valores dinámicos.
- Algunos códecs, particularmente los códecs de música, basan su compresión un conjunto de tramas sin comprimir y otros comprimidos aisladamente. En estos casos el codificador necesita tener algunas tramas anteriores de audio, o almacenarlos en un buffer un conjunto de ellas para su posterior reproducción. En otros casos, los códecs orientados a la voz suprimen el silencio, de tal forma que detectan y eliminan tramas que contienen solo silencio o ruido de fondo.

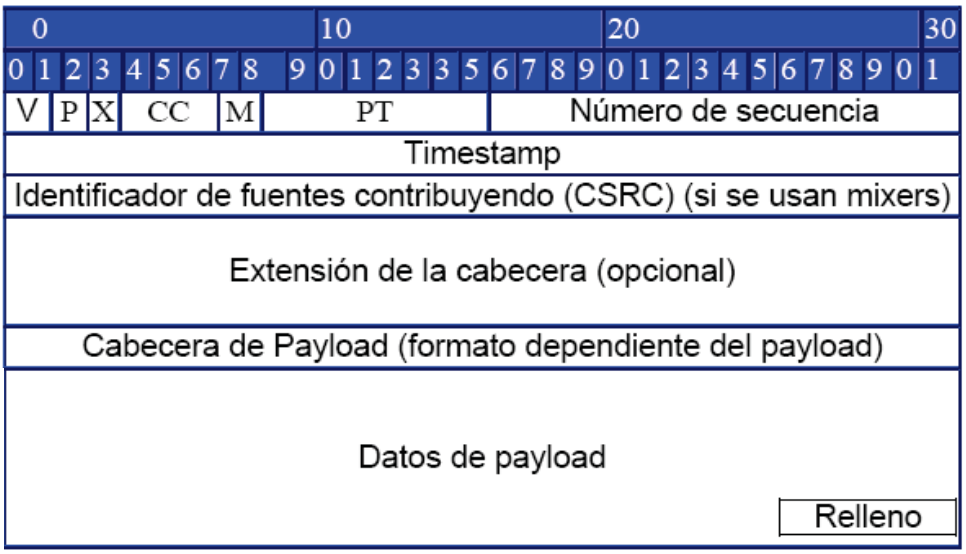
Captura multimedia y compensación: Vídeo



Captura del vídeo

- Los dispositivos de captura de vídeo funcionan normalmente sobre frames completos del video, en vez de devolver las líneas escaneadas individualmente o campos de una imagen entrelazada. Muchos brindan la posibilidad de submuestrear y capturar parte de un frame o devolver un subconjunto de los frames. Los frames pueden tener un rango de tamaños, y las capturadotas pueden devolver frames en variedad de formatos, espacios de color, profundidades, y subsampling.
- Dependiendo del códec usado, podría ser necesario convertir del formato usado a otro para poder ser visualizado. P.E. De RGB a YUV.
- En cuanto los frames de video han sido capturados, son almacenados antes de ser pasados al codificador para la compresión. El número de frames que son almacenados depende de qué esquema de compresión esté siendo usado; la mayoría de los códecs de video llevan a cabo la compresión interframe, esto es que cada frame depende de los frames circundantes. La compresión interframe puede exigir que el codificador retrase la compresión de un frame especial hasta que los frames de los que depende hayan sido capturados.

Generación de paquetes RTP:

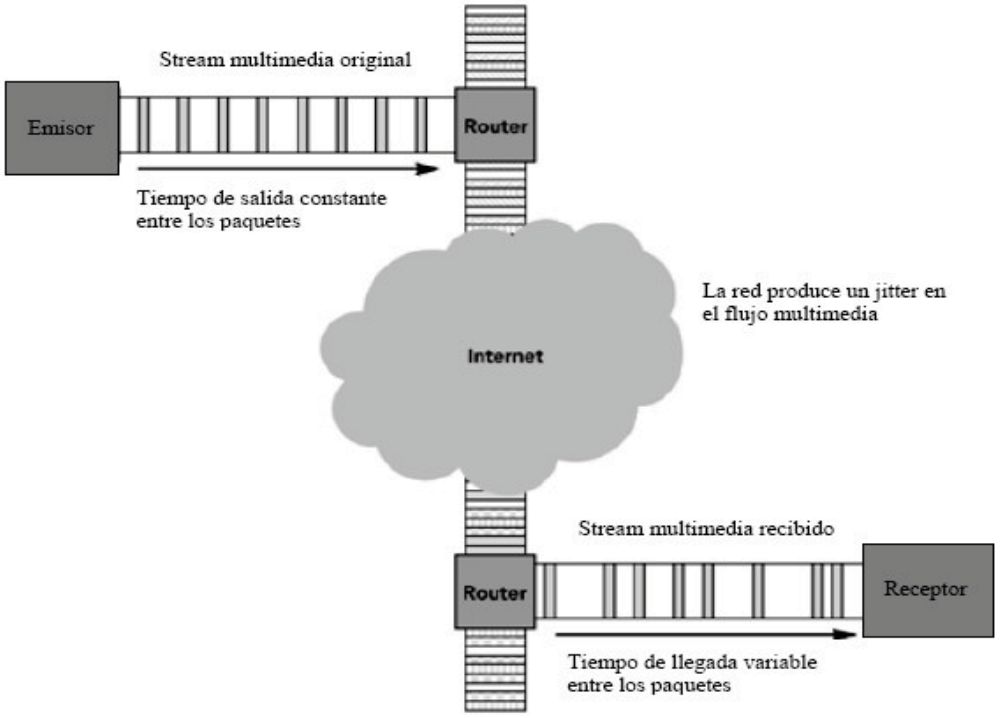


V: Número de la versión
P: Relleno
X:Extensiones
CC: Contador de fuentes contribuyendo
M: Marca
PT: Tipo de payload

Generación de paquetes

- Una vez que los frames son generados se pasan a la rutina de empaquetamiento RTP. Cada frame tiene asociado un timestamp, de la cual se obtiene la marca de tiempo de RTP. Si el payload soporta fragmentación, los frames grandes serán fragmentados en diferentes tramas. Para finalizar se generan uno o más paquetes RTP por cada frame, incluyendo cada uno los datos multimedia y cualquier cabecera de payload. El formato del paquete multimedia y la cabecera de payload son definidos de acuerdo con el formato de payload que se especifique para el códec. Las partes críticas para el proceso de generación de paquete son la asignación de timestamps a los frames, la fragmentación de frames grandes, y la generación de la cabecera de payload.
- Además de los paquetes de datos de RTP que representan a los frames directamente, el emisor puede generar paquetes de corrección de errores y puede reordenar frames antes de la transmisión. Una vez que son enviados los paquetes, los datos multimedia guardados en la memoria intermedia son liberados. El emisor no debe eliminar los datos que puedan ser necesitados para algún reenvío. El requisito para poder guardar o no esos datos durante algún tiempo, dependerá del códec y el esquema de rectificación de error usado.

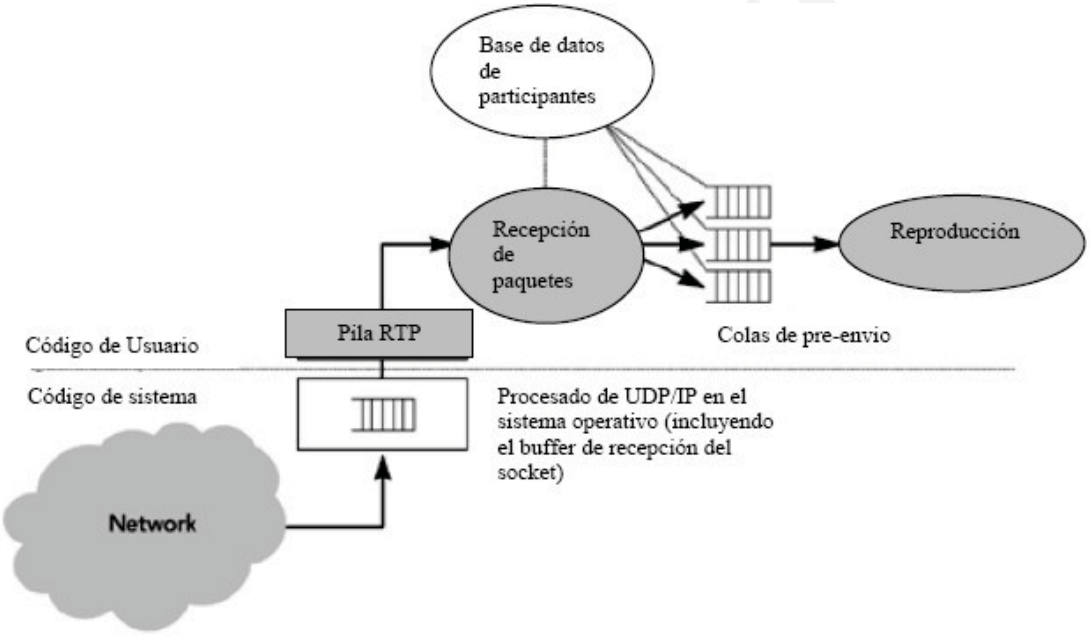
Recepción de paquetes (I):



Recepción de paquetes

- El primer paso del proceso de reproducción multimedia será capturar los paquetes de datos de RTP de la red, y almacenarlos en un buffer para su posterior proceso. La red puede afectar el cronometraje entre los paquetes, como muestra la siguiente figura, habrá saturación cuando varios paquetes lleguen a la vez o saltos cuando no llegue ningún paquete, además de que estos pueden llegar desordenados. El receptor no sabe cuándo van a llegar los paquetes con lo cual debe estar preparado tanto para las saturaciones como para los paquetes fuera de orden.
- Cuando los paquetes son recibidos, se valida para la corrección de errores, se anota su tiempo de llegada, y son añadidos a una cola de entrada, clasificada por fecha de RTP, para su posterior procesamiento.

Recepción de paquetes (y II):



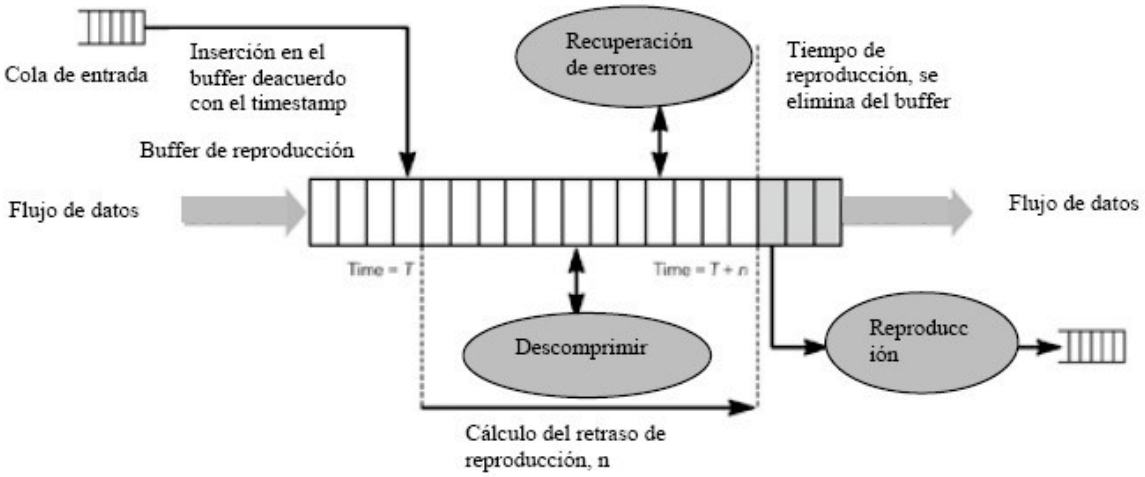
Recepción de paquetes

- Es importante almacenar el tiempo de llegada exacto de los paquetes de datos, M, con elpropósito de que pueda ser calculado el interarrival jitter El tiempo de llegada es inexacto ya que a las mediciones se le suma el jitter de la red y por ello se puede causar el retraso en la reproducción. El tiempo de llegada debe ser medido de acuerdo con la referencia local del reloj del sistema, T, convertido a la frecuencia del reloj multimedia, R. Es posible que este reloj no tenga esta funcionalidad y por lo tanto se calcula a través de la fórmula de la siguiente manera:

  M = T x R + offset

- Donde offset es usado para transformar el reloj de referencia al tiempo multimedia, ya que en el proceso de la corrección se puede distorsionar el reloj del tiempo multimedia con respecto al otro.

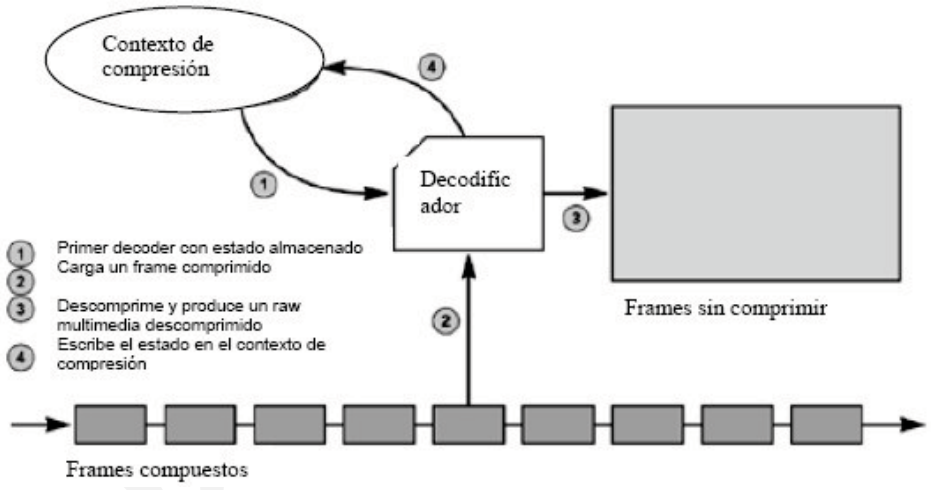
Decodificación, Mezclado y Reproducción: Decodificando (I)



Decodificación

- Los paquetes de datos son extraídos del buffer de entrada y son insertados en la memoria intermedia del reproductor (ordenadas igualmente por fecha de RTP). Los frames se almacenan aquí por un corto periodo de tiempo para suavizar las diferencias de cronometraje entre las diferentes tramas almacenadas así como para que lleguen todos los fragmentos de una trama fragmentada en el emisor o que llegue la corrección de algún fragmento. Entonces las tramas se descomprimen, cualquier error que quedara se detecta y se trata y se muestra el resultado al usuario.
- Con un único buffer se compensa la variabilidad de cronometraje de la red así como ser usado como memoria intermedia para el códec. Es posible separar estas funciones de forma que se usen buffers separados para compensar el jitter de la red y para la decodificación. El buffer del reproductor está formado por una lista ordenada por tiempo RTP. Cada nodo de la lista es un frame de datos multimedia con un tiempo asociado. La estructura también contiene un puntero a los nodos adyacentes, el momento de la llegada (tiempo de RTP), el tiempo de reproducción deseado para ese frame y punteros para los fragmentos comprimidos del frame (los datos recibidos en los paquetes RTP) y para la información multimedia descomprimida.

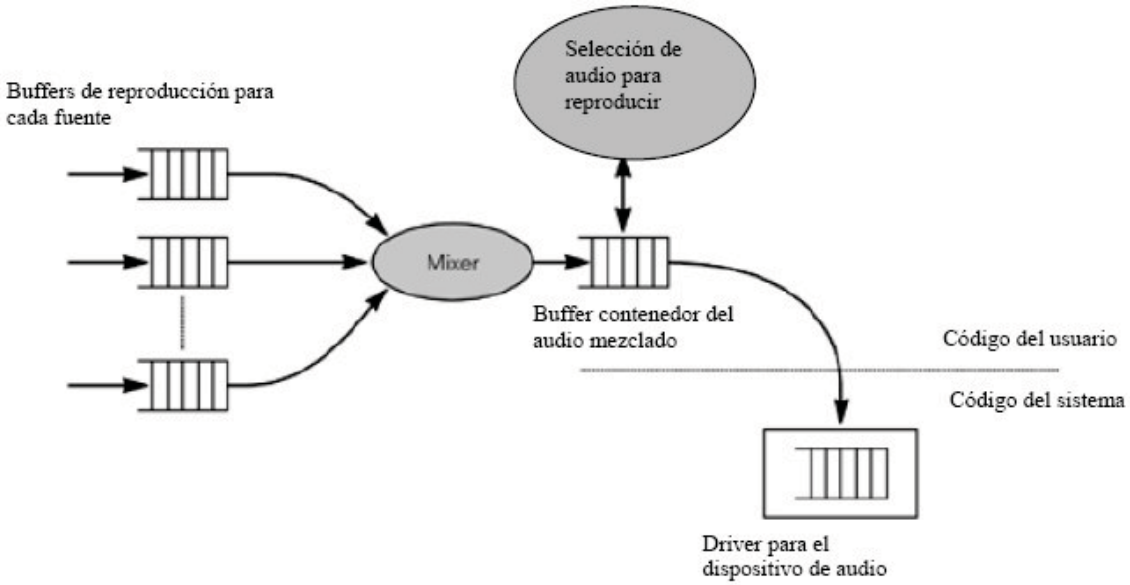
Decodificación, Mezclado y Reproducción: Decodificando (y II)



Decodificando (II)

- Para cada fuente activa la aplicación debe mantener una instancia del decodificador, comprendiendo tanto las rutinas de descompresión como el contexto de compresión con el que se creo el flujo multimedia. Cuando cada frame es descodificado, el contexto de compresión se refresca.
- El uso de un contexto de descompresión exacto es fundamental para que el descodificador opere correctamente ya que los códecs producirán resultados incorrectos si el contexto se pierde o es erróneo. Esto se produce a menudo si alguno de los paquetes de datos se pierde ya que habrá algunos frames no podrán ser descodificados. El resultado será un salto en la reproducción ya que no se podrá reproducir el frame que iría en ese lugar, además el contexto de descompresión será invalidado y los siguientes frames estarán corruptos.
- Dependiendo del códec es posible que se pueda señalizar que el frame se ha perdido, permitiendo al descodificador reparar lo mejor posible el contexto de forma que se minimicen el daño al flujo multimedia (por ejemplo muchos códecs orientados a la voz eliminan frames cuando detectan pérdidas en la señal). De otra manera el receptor deberá intentar reparar el contexto y ocultar los efectos de la pérdida

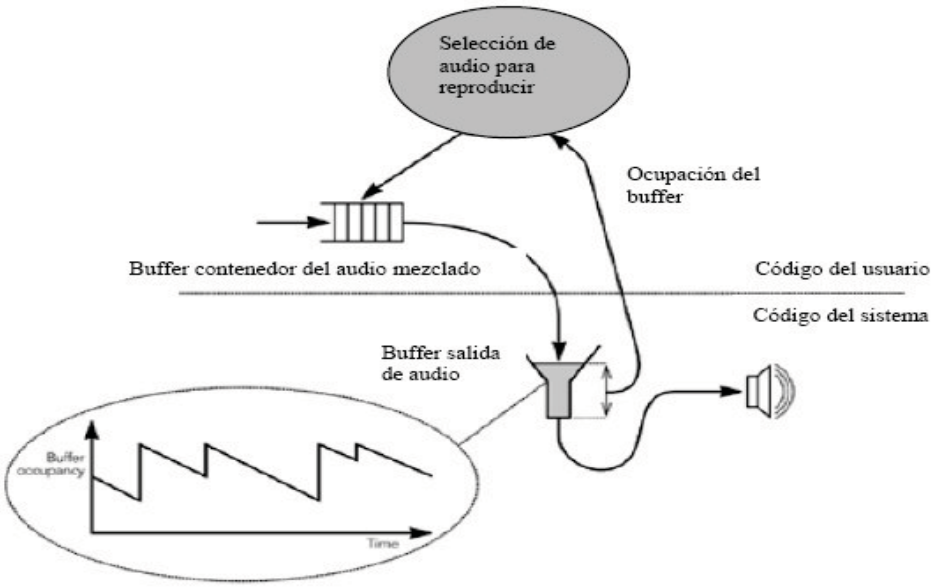
Decodificación, Mezclado y Reproducción: Mezclado



Mezclando el audio

- La mezcla (o mixing) es el proceso de combinar múltiples flujos multimedia en uno. Esto se suele dar sobre todo en el audio ya que la mayoría de los sistemas tienen un único juego de altavoces y múltiples fuentes activas, como es el caso de de una teleconferencia múltiple. Una vez que los flujos de audio han sido descodificados, se deben mezclar entre sí antes de ser enviado el producto final al dispositivo de audio. Las fases finales de una aplicación de audio se pueden estructurar como se muestra a continuación. El descodificador genera los datos de audio sin comprimir por cada fuente de datos, se almacenan en un buffer de reproducción distinto por cada fuente y el mezclador combina los resultados en un único buffer para la reproducción.
- Estos pasos pueden ocurrir en cualquier momento cuando el flujo de datos ha sido decodificado y antes de que llegue el momento de la reproducción.

Decodificación, Mezclado y Reproducción: Reproducción



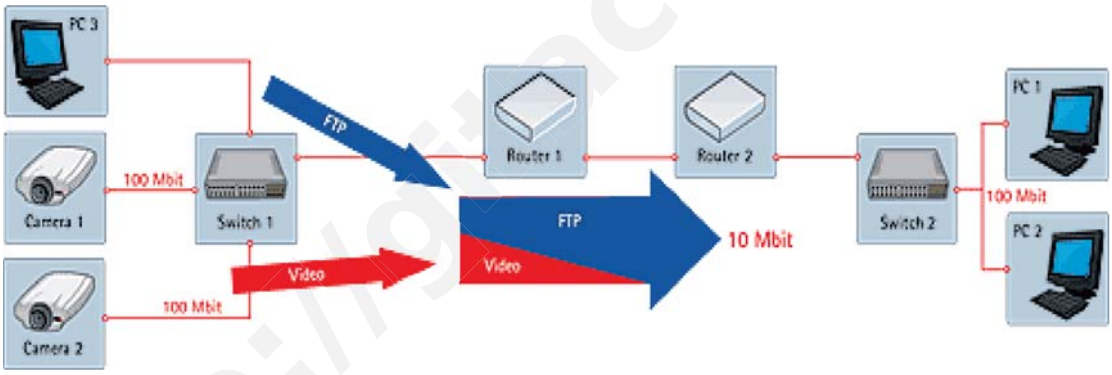
Reproducción de audio

- El proceso por el cual el audio es reproducido al usuario es normalmente asíncrono, permitiéndola sistema que a la vez que reproduce un frame puede estar procesando el siguiente.
- Esta capacidad es esencial para un modo de operar normal y corriente como el que estamos acostumbrados ya que de esta manera se puede estar reproduciendo ininterrumpidamente aunque la aplicación esté ocupada con la captura y el procesamiento de paquetes RTP.
- La reproducción asíncrona es especialmente importante sobre los sistemas operativos con un soporte para multimedia limitado. Estos sistemas son diseñados para proporcionar una buena reacción media ante los eventos, pero a menudo tienen un comportamiento bastante malo con respecto a este tipo de reproducciones. Una aplicación puede usar la reproducción asíncrona apoyándose en el hardware de audio, es decir en el DMA (Directory Memory Access) para conseguir una reproducción continúa. Una aplicación puede monitorear la ocupación del buffer de salida para ajustar la cantidad de información que se envía al dispositivo, de esa forma la ocupación del buffer después de cada iteración es continua.

Reproducción de vídeo

- La reproducción de vídeo es determinada por el refresco de la visualización, que determina el máximo tiempo entre la aplicación que está escribiendo en el buffer de salida y la imagen que está siendo presentada al usuario. La llave para conseguir una reproducción suave se consigue: (1) Los frames deben ser presentados con un refresco uniforme, y (2) los cambios realizados a un frame deben ser evitados mientras el vídeo está siendo renderizado.
  - El primer punto es un problema para el buffer de reproducción, ya que se debe seleccionar el tiempo apropiado para la visualización del vídeo.
  - El segundo punto está relacionado con la visualización en sí. Los frames no se muestran instantáneamente; en vez de eso se representan en series de líneas de derecha a izquierda, y de arriba abajo. Esta representación en serie permite la posibilidad de que la aplicación sea capaz de mostrar un nuevo frame mientras otro está siendo mostrado.

7. Protocolos para la provisión de QoS



Introducción

- IP fue diseñado para aplicaciones relativamente resistentes a:
  - Retardos
  - Variaciones en el rendimiento
  - Pérdidas de paquetes
- Inicialmente, la demanda de tráfico era modesta, también la capacidad de los enlaces.
- Hoy, IP debe soportar:
  - Aplicaciones sensibles a retardos, variaciones y pérdidas
  - Junto con aplicaciones convencionales
  - Cargas de tráfico mucho mayores y más heterogéneas
  - Sobre enlaces de capacidad también mayor

Modelos de servicio sobre IPv4

- IPv4 describe el modelo *best-effort*
  - Cada datagrama se trata como una entidad independiente
  - No existen conexiones ni circuitos lógicos
- Incorpora un campo TOS (*Type Of Service*) para el control de la provisión del servicio
  - Se establece una relación entre niveles de servicio y valores de TOS
  - No se describen los mecanismos a aplicar para proporcionar diferentes niveles de servicio
  - En la práctica, normalmente se ignora.

Modelos de servicio sobre IPv6

- IPv6 incluye un campo Traffic Class (TC)
  - Permite distinguir clases o prioridades de tráfico
  - Incluido por compatibilidad con TOS de IPv4
  - No se establece una asignación de valores
  - No se describen los mecanismos a aplicar para proporcionar diferentes niveles de servicio
  - En la práctica, normalmente también se ignora.

Quality of Service (QoS)

- En el contexto de las redes de conmutación de paquetes, el término *Quality of Service* (QoS) se refiere al conjunto de mecanismos de control que:
  - Puedan proporcionar prioridades distintas a usuarios o a flujos de datos distintos
  - Garanticen el cumplimiento de ciertos parámetros en un rango para un flujo de datos de acuerdo con las peticiones de la aplicación o de la política del ISP.
- Las garantías de QoS son importantes si la capacidad de red está limitada, por ejemplo en comunicaciones de datos móviles.
- Especialmente para aplicaciones multimedia, como VoIP, IPTV, etc.

Parámetros QoS sobre IP

- Retardo o *delay*
  - Tiempo de llegada de un datagrama desde que es enviado
  - Retardo medio y retardo máximo
- Variabilidad o *jitter*
  - Variación sobre el retardo medio
- Throughput
  - Cantidad de datos por unidad de tiempo
  - Throughput medio y throughput máximo
- Fiabilidad o *reliability*
  - Tasa media de error extremo a extremo de la red

Provisión de garantías QoS

- Para que una red IP pueda proporcionar garantías QoS, es necesario, al menos:
  - Añadir funcionalidad a los *router*
  - Incorporar mecanismos para solicitar QoS
- Algunos conceptos:
  - Especificación de las acciones en la red: **clases de servicio**
  - Especificación de un conjunto de clases de servicio: **modelo de servicio**
  - *Service Level Agreement* (*SLA*)
  - *Traffic Contract Agrement* (*TCA*)

Provisión de garantías QoS en Internet

- ¿Es realmente necesario? ¿Y si...?
  - ¿Ancho de banda infinito?
  - ¿Aplicaciones adaptativas?
  - ¿Priorización de flujos?
- Diferenciar esquemas de tráfico como un Servicio de Valor Añadido (SVA)
- Internet + garantías de calidad de servicio (QoS):
  - Se podría crear una red paralela QoS
  - Se perderían las ventajas de compartición estadística BE + QoS
  - Más complejo de construir y administrar

Definición de Flujo

- Un paquete IP puede asociarse con un flujo:
  - Secuencia distinguible de paquetes IP
  - De la actividad de un único usuario
  - Que requiere la misma QoS
  - Unidireccional, aunque puede tener más de un destino (multicast)
  - La pertenencia de un paquete a un flujo se determina mediante un clasificador multicampo:
    - Dirección IP origen
    - Dirección IP destino
    - Números de puerto
    - Tipo de protocolo
  - O también mediante el TC de IPv6

Tráfico elástico

- Puede ajustarse a cambios en *delay* y *throughput*.
- Ejemplo: aplicaciones TCP y UDP convencionales:
  - E-Mail – insensible a *delay* y *jitter*.
  - FTP – sensible a únicamente a cambios en *throughput*.
  - SNMP – insensible al *delay*, excepto cuando está causado por la congestión.
  - Web (HTTP), TELNET – sensibles al *delay*.
- *Delay* por paquete / tiempo total empleado
  - Ej.: Tiempo de carga de una página web.
  - Objetos pequeños: *delay* es importante.
  - Objetos grandes: *throughtput* sobre *delay*.
  - For large items it is throughput over connection
- Se necesita cierto control QoS acorde a las demandas.

Tráfico no elástico

- No se adapta fácilmente a cambios en *delay* y *throughput*
  - Tráfico en tiempo real
- *Throughput*
  - Se podría requerir un mínimo
- *Delay*
  - Ej.: Operaciones sobre Bolsa
- *Jitter* (variación de *delay*)
  - Más *jitter* : *búffers* más grandes
  - Ej. En teleconferencia se requiere un límite superior razonable.
- Pérdida de paquetes

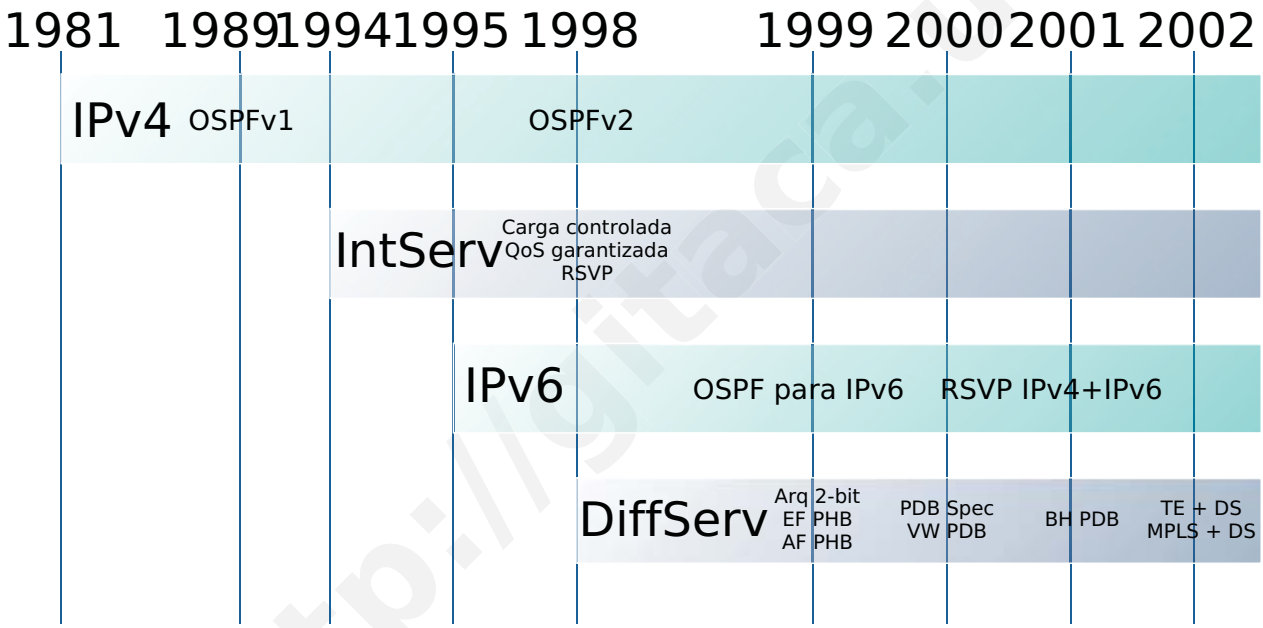
Problemas asociados al tráfico no elástico

- Dificultad para cumplir los requierimientos en una red con *delays* de *queuing* variables y con congestión.
- Necesita tratamiento preferente
- Las aplicaciones deben indicar sus requerimientos
- ...y además coexistir con el tráfico elástico (¡que estaba antes!)
  - Denegar peticiones de servicio que dejarían demasiados pocos recursos como para poder transportar tráfico elástico.

Modelos de servicio

- Best-effort (BE): el más popular
- Red Telefónica: asignación de circuitos
- Otros modelos:
  - Servicios Integrados (IntServ)
  - Servicios Diferenciados (DiffServ)
  - ATM

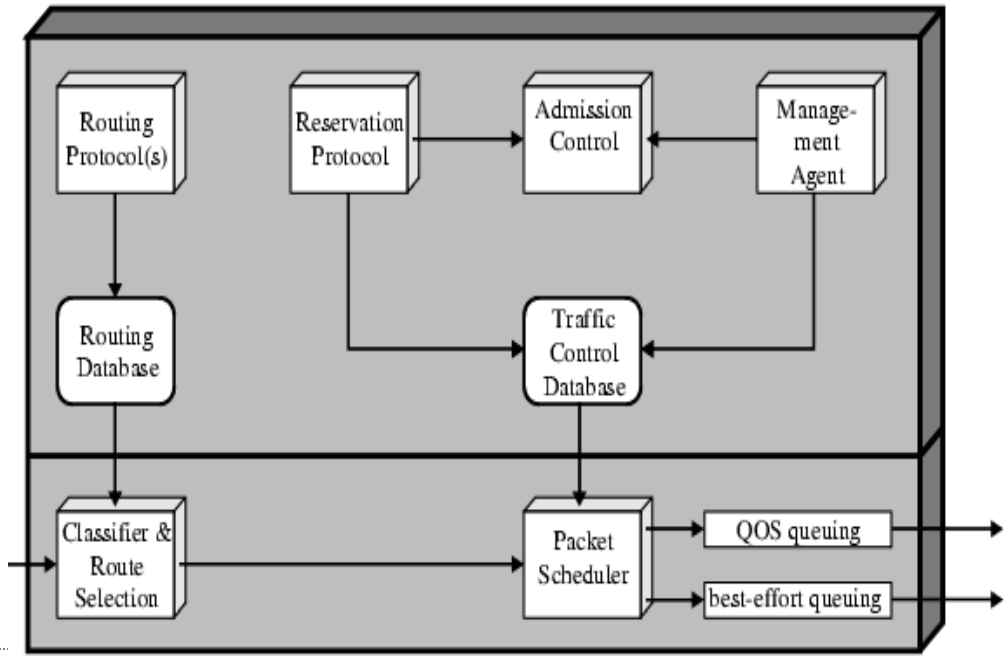
Modelos de servicio en Internet



Modelo de Servicios Integrados (IntServ)

- Para realizar garantías, los *router* deben reservar recursos
  - Existencia de estados no sólo en los extremos de la comunicación; también en los *router*
  - Control de acceso
  - Autentificación de paquetes
- Nuevos componentes en los *router*:
  - Planificador de paquetes
  - Clasificador
  - Control de admisión

IntServ – Componentes del control de tráfico



IntServ – Niveles de servicio

- Servicio de carga controlada
  - Reservas estadísticas, no estrictas
    - La tasa de error extremo a extremo aprox. igual a la tasa de error del medio de transmisión
    - Retardo medio no excede significativamente el retardo mínimo
  - Adecuado para aplicaciones sensibles a condiciones de congestión en la red
- Servicio de QoS garantizada
  - Reservas estrictas
  - Retardo máximo acotado, pero no controla *jitter*
  - Retardo medio mucho menor que retardo máximo

IntServ – Problemática asociada

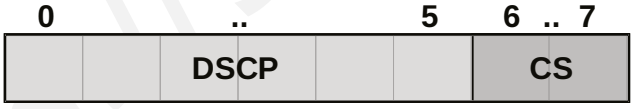
- Información de estado en *router* proporcional a número de flujos: baja escalabilidad
- Elevados requerimientos en *router*
- Implantación completa
- Garantías de retardo no útiles para flujos de bajo *throughput*
- Modificación de las aplicaciones para realización de reservas

Modelo de Servicios Diferenciados (DiffServ)

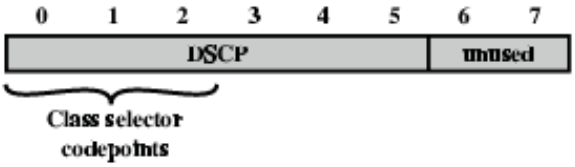
- Búsqueda de soluciones más simples que IntServ
- ¿Necesidad de provisión de garantías estrictas?
- DiffServ:
  - El servicio por flujo se reemplaza por un servicio por agregación
  - El procesamiento complejo se desplaza de los *core router* a los *edge router*

DiffServ – Campo DS

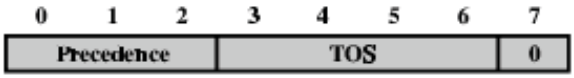
- Clasificación de los flujos
  - Realizada en *host* o *ingress router*
  - A clases agregadas
  - Clase del paquete se marca en la cabecera
  - *Core router* no clasifican por flujos
- Marcación de paquetes: campo DS
  - Almacenado en TOS (IPv4) / TC (IPv6)



DiffServ – Campo DS vs IPv4 ToS



(a) DS Field



Precedence		TOS Subfield	
111	Network control	1000	Minimize delay
110	Internetwork control	0100	Maximize throughput
101	Critical	0010	Maximize reliability
100	Flash override	0001	Minimize monetary cost
011	Flash	0000	Normal service
010	Immediate		
001	Priority		
000	Routine		

(b) IPv4 Type of Service Field

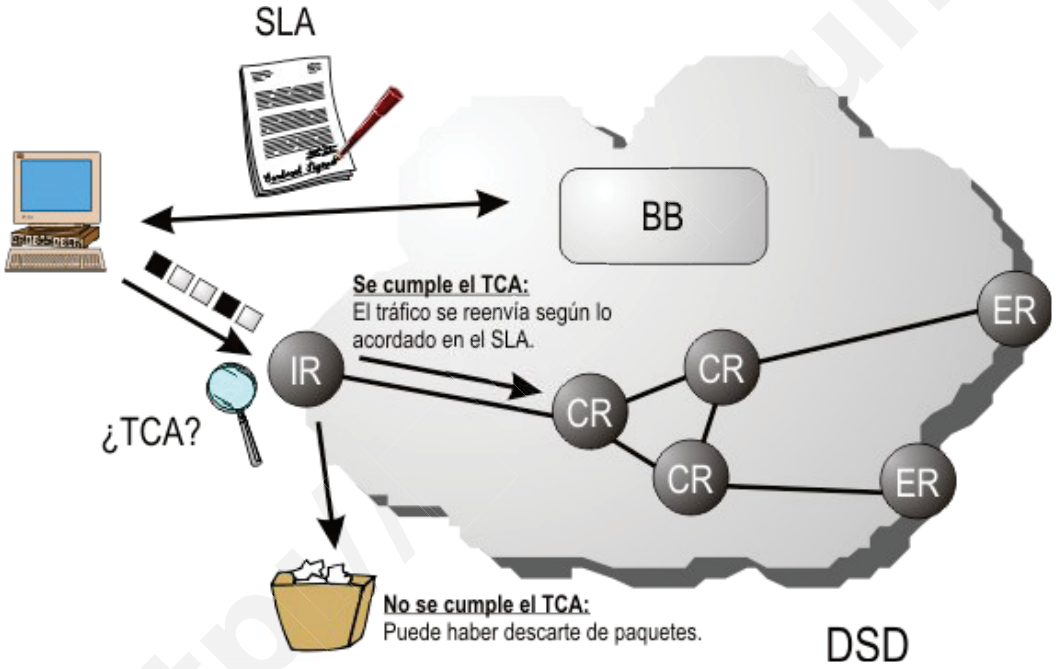
DiffServ – Per-Hop Behaviors (PHB)

- PHB: actuación de un nodo DiffServ ante una colección de paquetes con el mismo DSCP
- Tres tipos:
  - PHB Implícito
    - Tratamiento BE: garantiza fiabilidad
  - PHB de envío rápido (EF PHB)
    - Garantiza retardo, jitter, throughput y fiabilidad
  - PHB de envío asegurado (AF PHB)
    - Garantiza throughput y fiabilidad

DiffServ – Bandwidth Broker (BB)

- Deben asignarse y controlarse los recursos de la red
- Asignación manual: sólo para casos muy simples
- Integración de un agente (llamado Bandwidth Broker o BB) que:
  - Asigna tráfico a *router*
  - Establece parámetros de clasificación y planificación de paquetes
  - Mantiene una BD de control de acceso
  - Realiza control de admisión

DiffServ – Service Level Agreement



Ingeniería de Tráfico

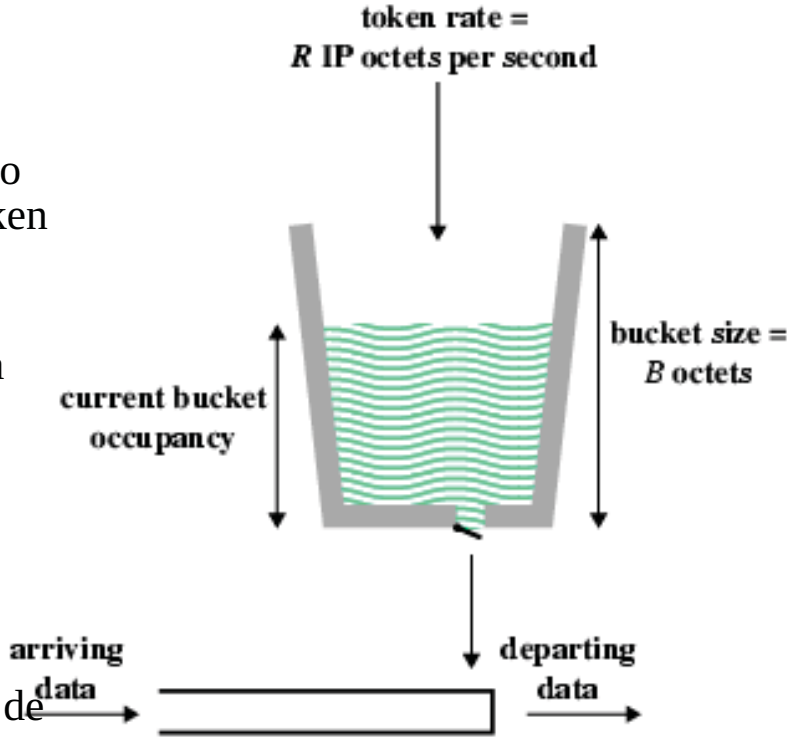
- Ingeniería de tráfico (TE) en Internet:
  - Evaluar y optimizar el rendimiento de redes operativas
- Complemento a DiffServ
- Mecanismos TE útiles para DiffServ:
  - Encaminamiento basado en restricciones (CBR)
  - QoS Routing (QoSR)
  - Multi Protocol Label Switching (MPLS)

Ingeniería de Tráfico – CBR y QoSR

- Obtención de QoS: CBR resulta útil si se considera retardo y *jitter*
  - Gran coste computacional
  - Online: heurísticas para soluciones razonables
  - Offline: intervención humana y cálculo de soluciones globales óptimas
- QoSR: búsqueda de rutas para alcanzar los parámetros QoS requeridos
  - Si los algoritmos convencionales devuelven una ruta adecuada, utilizarla
  - Si no, realizar búsqueda de caminos según los requerimientos de QoS

Token Bucket

- Se puede describir el comportamiento de muchas fuentes de tráfico mediante el esquema token bucket.
- Proporciona una descripción precisa de la carga impuesta por un flujo.
  - Es más sencillo determinar requerimientos de recursos.
- Proporciona parámetros de entrada a la función *policy*



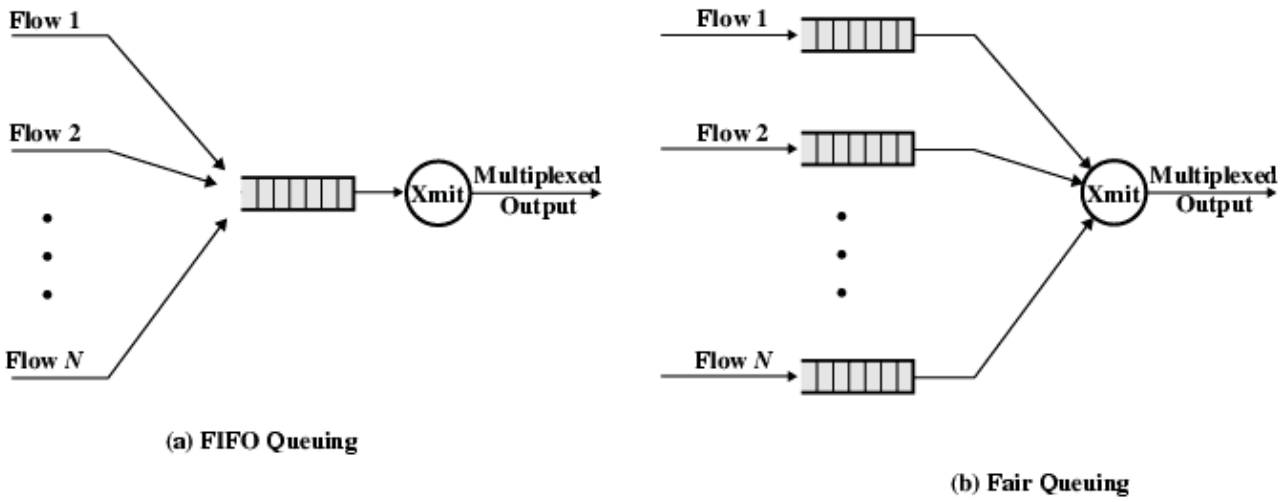
Disciplina de queuing

- Tradicionalmente, la disciplina de *queuing* utilizada en cada puerto de cada *router* es FIFO (*First In First Out*) ó FCFS (*First Come First Served*).
- No se proporciona tratamiento especial a los paquetes (flujos) de alta prioridad.
- Los paquetes cortos son retenidos por los paquetes largos que se encuentren delante en la *queue*.
  - El *delay* medio para los paquetes cortos se incrementa.
  - Los flujos de paquetes largos obtienen un mejor servicio.
- Las conexiones TCP voraces relegan otras conexiones más “altruistas”.

Fair Queuing (FQ)

- Varias *queues* por puerto:
  - Una *queue* por cada fuente o flujo.
  - Las *queues* se despachan en *Round Robin.*
  - Se despacha exactamente un paquete por ciclo en cada *queue* ocupada.
  - La carga se balancea entre los flujos.
  - Aunque las conexiones sean voraces, no obtienen ninguna ventaja.
    - Las *queues* se vuelven más largas y el *delay* medio se incrementa.
  - Se penaliza a los paquetes cortos, ya que se transmite un paquete por ciclo

FIFO y FQ



(a) FIFO Queuing

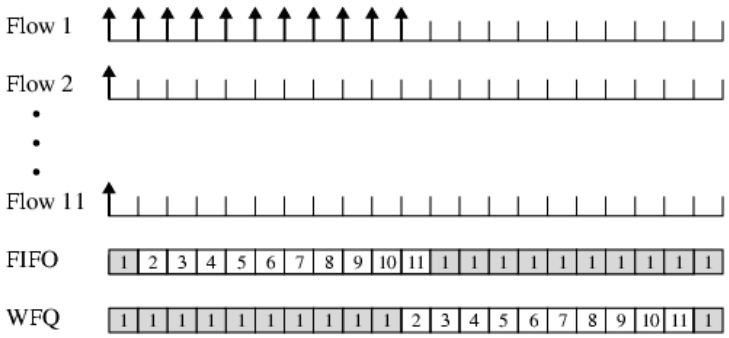
(b) Fair Queuing

Processor Sharing

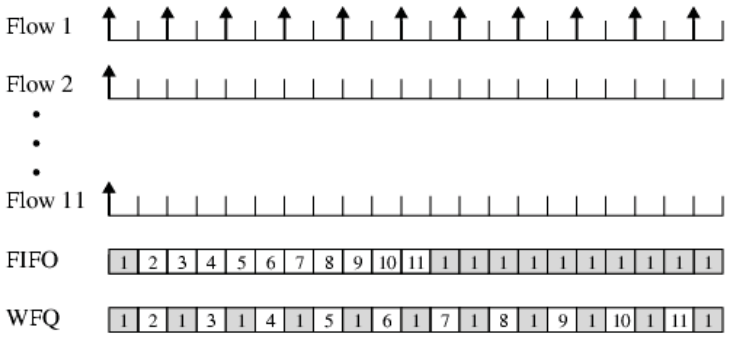
- Varias *queues*, como en FQ.
- Se envía un bit de cada *queue* por turno.
  - De este modo, los paquetes más largos no obtienen ventaja.
- Puede determinarse los tiempos *virtuales* de comienzo y fin (número de ciclos) para un paquete dado.
- En cualquier caso, queremos transmitir paquetes, no bits.

Generalized Processor Sharing (GPS)

- Partiendo de PS, se asigna una *ponderación* a cada flujo, que determina cuántos bits pueden enviarse en cada turno.
  - Si la ponderación es 5, entonces se transmiten 5 bits por turno.
- Proporciona un modo de diferenciar niveles de servicio.
- Garantiza que el *delay* no excede un límite.
- Extensión denominado *Weighted fair queue* (*WFQ*).
  - Emula GPS bit a bit.



(a)



(b)

Descarte proactivo de paquetes

- Control de la congestión mediante descarte proactivo de paquetes.
  - Antes de que se llene el búffer.
  - Se utiliza sobre una sóla *queue* FIFO o sobre varias *queues* para tráfico elástico.
  - Ej. Random Early Detection (RED)

Random Early Detection (RED): Motivación

- La detección de pérdida de paquetes en TCP es una señal para entrar en la fase de *slow start*, reduciendo la carga.
  - Se deben reenviar los paquetes perdidos:
    - Incrementando carga y *delay*.
  - Sincronización global:
    - Las ráfagas de tráfico llenan las *queues*, provocando pérdidas de paquetes.
    - Muchas conexiones TCP entran en fase de *slow start*
    - La carga de tráfico disminuye, provocando infrautilización de la red.
    - Las conexiones abandonan la fase *slow start* simultáneamente, provocando nuevas ráfagas.
- Aumentar el tamaño de los búffer no ayuda.

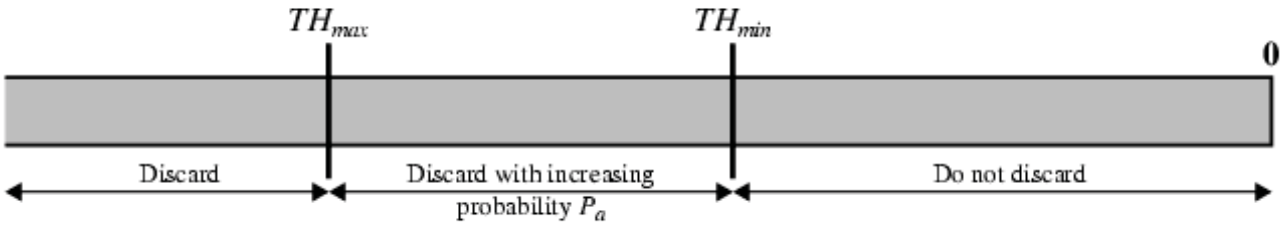
Objetivos de diseño de RED

- Evitar la congestión.
- Evitar la sincronización global.
- Evitar que el tráfico se vuelva a ráfagas.
- Se mantiene un tamaño medio de las *queues*.
  - Controlando de este modo el *delay* medio.

Algoritmo RED

```
Calculate average queue size avg
  if avg < THmin
     queue packet
  else if THmin ≤ avg < Thmax
     calculate probability Pa
     with probability Pa
          discard packet
     else with probability 1-Pa
          queue packet
  else if avg ≥ THmax
     discard packet
```


Búffer RED



Algoritmo RED en detalle

Initialization:
  $avg \leftarrow 0$
  $count \leftarrow -1$
For each packet arrival
  CALCULATE AVERAGE QUEUE SIZE
    if the queue is not empty (i.e., $q > 0$)
      $avg \leftarrow (1 - w_q)avg + w_q q$
    else
      $m \leftarrow f(time - q\_time)$
      $avg \leftarrow (1 - w_q)^m avg$
  DETERMINE PACKET DISCARD
    if $avg < TH_{min}$
      queue packet
      $count \leftarrow -1$
    else if $TH_{min} \leq avg \leq TH_{max}$
      increment $count$
      $P_b \leftarrow P_{max}(avg - TH_{min})/(TH_{max} - TH_{min})$
      $P_a \leftarrow P_b/(1 - count \times P_b)$
      with probability P_a
        discard packet
        $count \leftarrow 0$
      else with probability $1 - P_a$
        queue packet
    else if $avg > TH_{max}$
      discard packet
      $count \leftarrow 0$
When queue becomes empty
  $q\_time \leftarrow time$

Saved Variables:
- avg: average queue size
- q_time: start of queue idle time
- $count$: packets since last discarded packet

Fixed Parameters:
- w_q: queue weight
- TH_{min}: Minimum threshold for queue
- TH_{max}: Maximum threshold for queue
- P_{max}: Maximum value for P_b

Other:
- P_a: current packet-marking probability
- P_b: temporary probability used in calculation
- q: current queue size
- $time$: current time
- $f(t)$: a linear function of time t

Administración Avanzada de Redes TCP/IP

MPLS: descripción

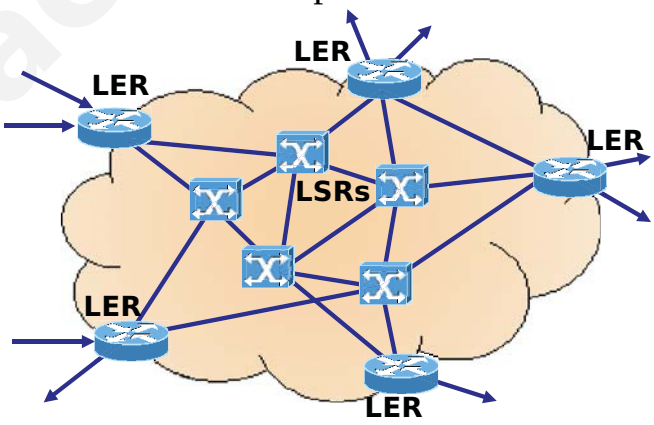
- Propuesta IETF para Label switching:
- Propuesta de nombres para label switching:
  - Ipsilon: IP switching
  - Cisco: Tag switching
  - Toshiba: Cell switching
  - Lucent: IP Navigator
- IETF: MPLS (RFC 3031, Enero 2001)
- Base: Marcado y gestión de paquetes por el LSR (Label Switching Routers):
- Se añaden etiquetas en el ingress router (incoming) “label push” y para el egress router (outgoing) “label pop”

MPLS: descripción

- MPLS actúa entre la capa de enlace y la de red
- Circuitos virtuales LSP (Label Switched Path):
  - Es una conexión MPLS entre dos LSR
- Cada nodo de la red realiza las siguientes funciones:
  - Reenvían (forward) paquetes únicamente en función de las etiquetas
  - Hacen swaping de etiquetas en los paquetes cuando son conmutados
  - Desde una interfaz de entrada a la de salida

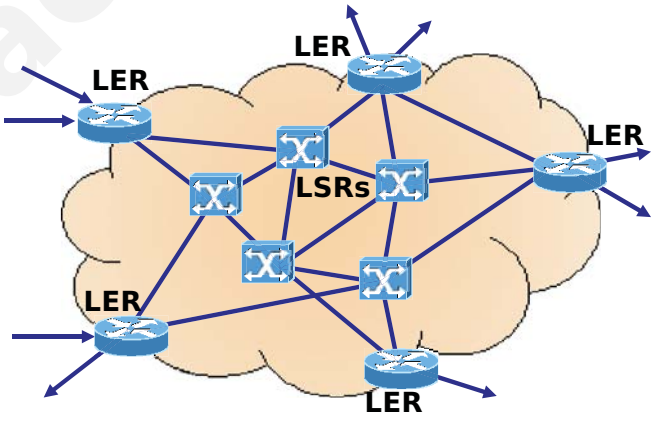
MPLS: componentes

- Routers LER (Label Edge Router) actúan de interfaz con otras redes y están situados en la frontera de la red MPLS. Se clasifican en nodos de entrada (ingress node) y de salida de la red MPLS (egress node). Funciones:
  - Envían el tráfico entrante a la red MPLS mediante un protocolo de señalización de etiquetas.
  - Distribuyen el tráfico de salida hacia las redes destino.



MPLS: componentes

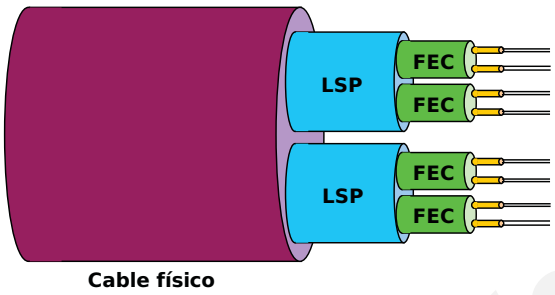
- Routers LSR (Label Switched Router) representan núcleo del backbone de la red. Son routers de gran velocidad. Funciones principales:
  - Participan en el establecimiento de los circuitos extremo-extremo de la red o LSP (Label Switched Path) mediante un protocolo de señalización.
  - Conmutan rápidamente el tráfico de datos entre los caminos establecidos.



MPLS: Clases de Reenvío Equivalente (FEC)

- FEC es el conjunto de paquetes con características comunes para facilitar su transporte ya que recibirán el mismo tratamiento hasta llegar al destino:
  - Cuando un paquete entre en la red se le asigna un FEC concreto.
  - Cada FEC representa unos requerimientos de servicio para un grupo de paquetes o para una dirección fija.
  - La clase FEC que se asigna a un paquete se codifica como un valor corto de longitud fija (etiqueta)
  - La etiqueta es usada por los conmutadores de la red para encaminar el paquete al siguiente nodo. La etiqueta viaja con el paquete
  - La etiqueta se usa en cada nodo como índice de acceso a la tabla que especifica el salto al siguiente router y una nueva etiqueta
  - La etiqueta de entrada es sustituida por la de salida y acompaña al paquete que es enviado al siguiente salto o router.

MPLS: Clases de Reenvío Equivalente (FEC)



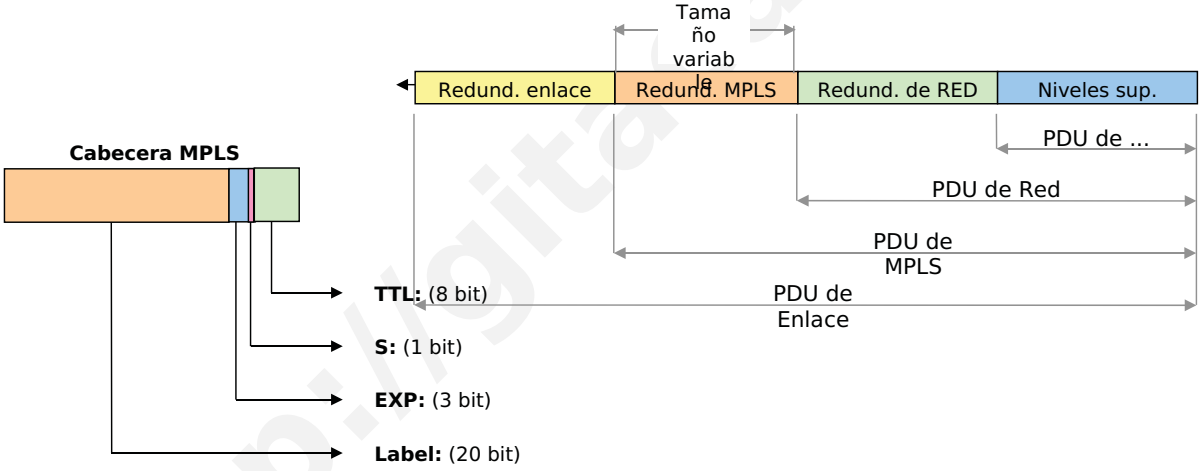
Relación FEC/LSP

Granulado grueso → sistema muy escalable pero no se podrían diferenciar tipos de tráfico y por tanto no permitiría clases de tráfico ni QoS. Ejemplo: FEC en la que se incluyeran todos los paquetes en los que la dirección destino coincidiera con un determinado prefijo.

Granulado fino → permite más clasificaciones de tráfico y mejor operación de QoS, pero a costa de especificar más FECs, necesitar más etiquetas y por tanto tabla de encaminamiento mayor.

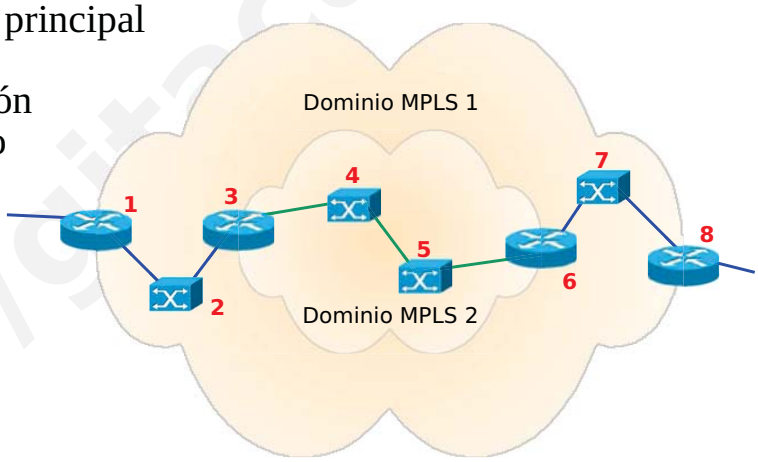
MPLS: formato de cabecera

- Encapsulado vs. Etiquetado.
- MPLS situado entre niveles de enlace y red (nivel 2+) del RM-OSI. Actúa como interfaz entre los distintos protocolos y el nivel de enlace.



Pila de etiquetas (Label Stack)

- El campo S indica el tipo de la siguiente cabecera. Si un paquete entra en un nuevo dominio sin salir antes de otro, se añade una nueva cabecera, pero con S=0 (si solo hay una etiqueta MPLS, entonces S=1).
- El LER de salida de cada dominio anidado se encarga de desapilar etiquetas. El del dominio principal encontrará S=1 y sabrá tratar el paquete en función del nuevo protocolo, pero ¿cómo lo hace?

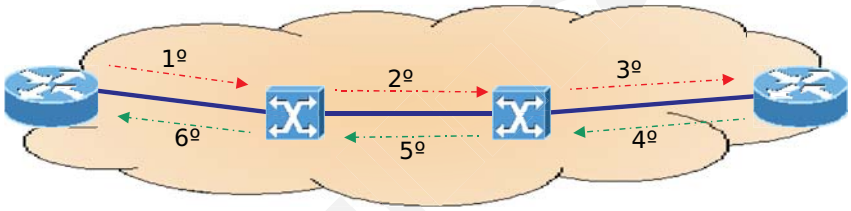


Nº 335

Administración Avanzada de Redes TCP/IP

Distribución de etiquetas

- LDP (Label Distribution Protocol): Suele emplear una asignación de etiquetas bajo demanda, trabajando en sentido contrario al flujo de datos.
- El resultado es un LSP por el que circularán todos los paquetes de un mismo flujo.

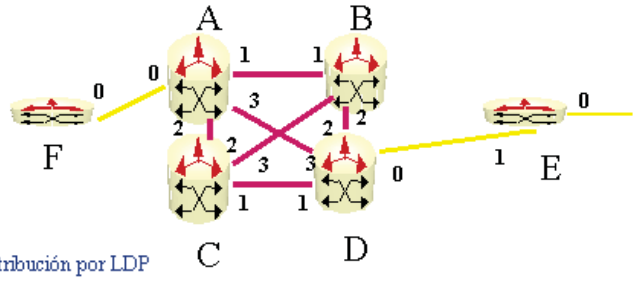


Distribución de etiquetas en upstream

- RSVP: Cobra ahora importancia al permitir establecer LSPs mediante reparto de etiquetas sobre una sesión RSVP previa.
- RSVP-TE: aporta nueva estrategia para la creación eficiente de LSPs en función de la carga actual del dominio, así como mecanismos de gestión de LSPs ya existentes.

Nº 336

Sea el dominio MPLS de la figura de la derecha, siendo F y E nodos LER y A, B, C y D nodos LSR. Tras la ejecución del protocolo de distribución de etiquetas LDP, la tabla FIB (Forwarding Information Base) queda como se muestra en la figura inferior. a) Indicar los pasos que se han seguido para obtener dicho reparto de etiquetas según LDP. b) Detallar los pasos que se siguen para el reenvío de un paquete a través del LSP=(F,A,D,E)



Entradas iniciales en FIB

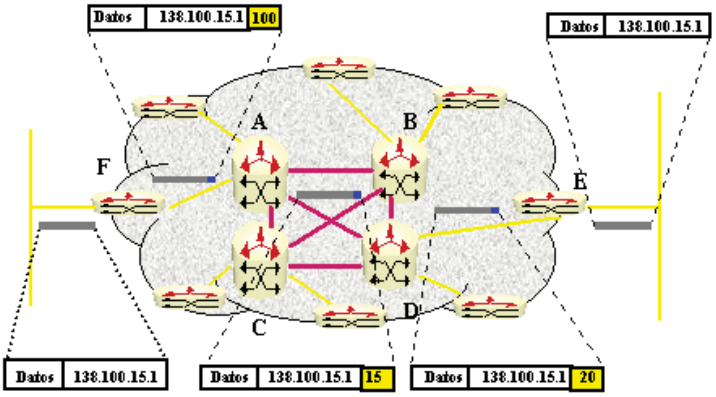
	Etiqueta Entrada	Etiqueta Salida	Próximo Salto	Interfaz Salida
LSR A	100	?	D	3
LSR B	10	?	D	2
LSR C	25	?	D	1
LSR D	15	?	E	0
LSR E	20	?	E	0
LSR F	-	?	A	0

Entradas en FIB tras distribución por LDP

	Entrada	Salida	Salto	Salida
LSR A	100	15	D	3
LSR B	10	15	D	2
LSR C	25	15	D	1
LSR D	15	20	E	0
LSR E	20	-	E	0
LSR F	-	100	A	0

Forwarding Information Base

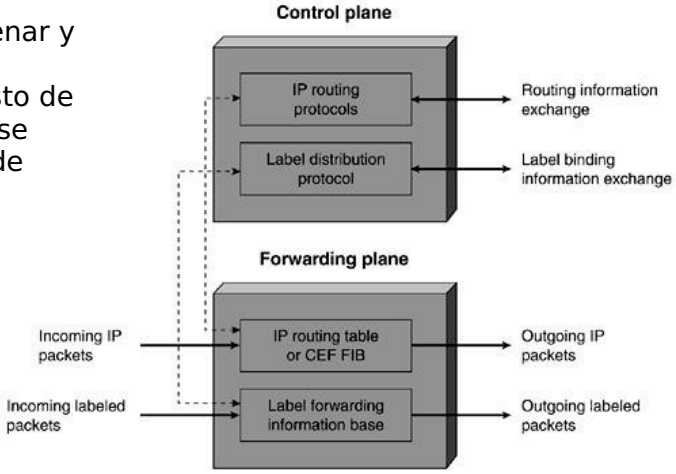
Conmutación de etiquetas a través de LSP=(F,A,D,E)



Nº 337

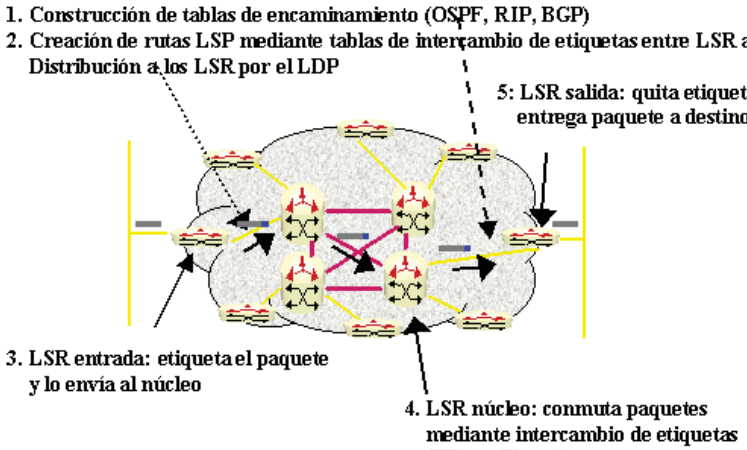
Arquitectura de un nodo MPLS

Plano de Control (PC) → responsable de rellenar y mantener la FIB. Se ejecuta un protocolo para intercambiar info de enrutamiento IP con el resto de nodos MPLS del dominio. La info de etiquetado se intercambia mediante un prot. De distribución de etiquetas. Las etiquetas intercambiadas con los vecinos se utilizan para construir la FIB.
Plano de Reenvío (PR) → responsable del reenvío de paquetes basado en el valor de las etiquetas. Utiliza la FIB creada y mantenida por el Plano de Control para esta tarea.



Nº 338

Arquitectura de un nodo MPLS



En la figura de la izquierda se muestra un resumen de la operación de MPLS en un dominio. Las tareas 1 y 2 son propias del PC y las 3, 4 y 5 las lleva a cabo el PR con la info proporcionada por el PC.

Aplicaciones de MPLS

- Integración de protocolos (¿solución al conflicto IPoATM?). MPLS permite cualquier protocolo de nivel superior (IP), pero también cualquier tecnología de nivel de enlace (ATM), por tanto: IPoMPLSoATM.
- Redes privadas virtuales. Puede hacerse coincidir un enlace privado virtual con un FEC/LSP particular.
- MPLS-TE. Balanceo de carga en el dominio, re-enrutado automático a un backup-LSP al detectar un fallo en el LSP actual, ...
- Calidad de Servicio extremo a extremo en el dominio. Se admite el empleo del campo EXP de la cabecera para clasificar el tráfico en clases de servicio. Esto condicionará el tratamiento que recibirá cada paquete a lo largo de todo el dominio.

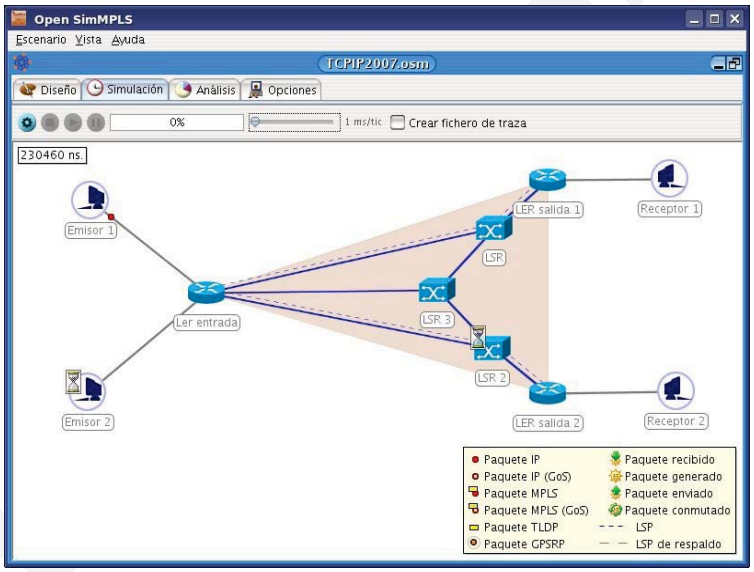
OpenSimMPLS v1.0

- Simulador de redes GoS/MPLS. Desarrollado por GITACA.
- Disponible en http://gitaca.unex.es/opensimmpls

Administración Avanzada de Redes TCP/IP

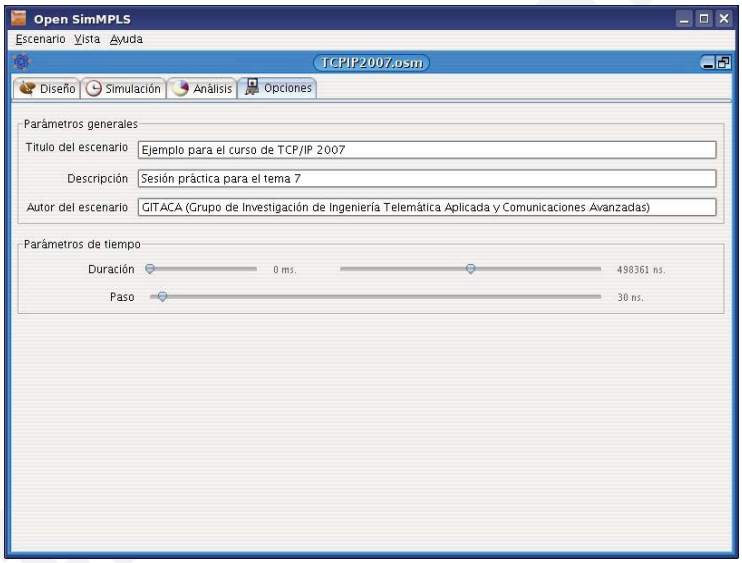
OpenSimMPLS v1.0

- Permite el diseño y simulación de redes MPLS.



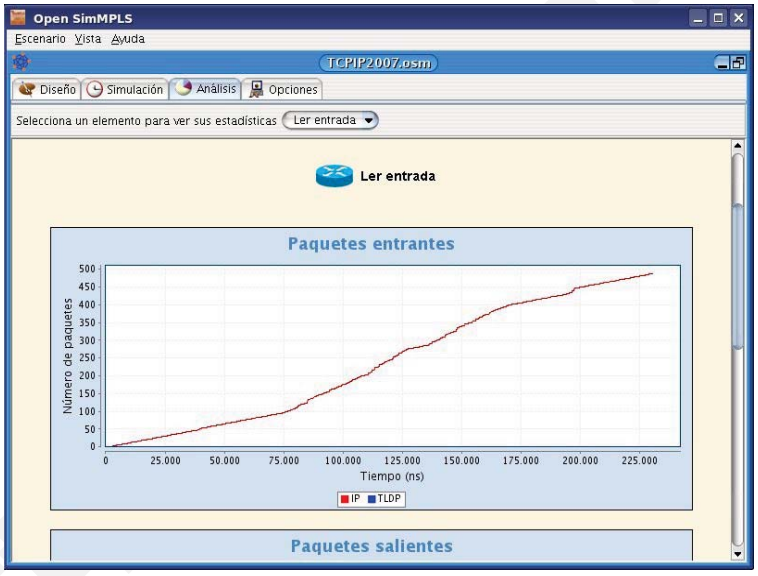
OpenSimMPLS v1.0

- Permite ajustar los parámetros de la simulación.

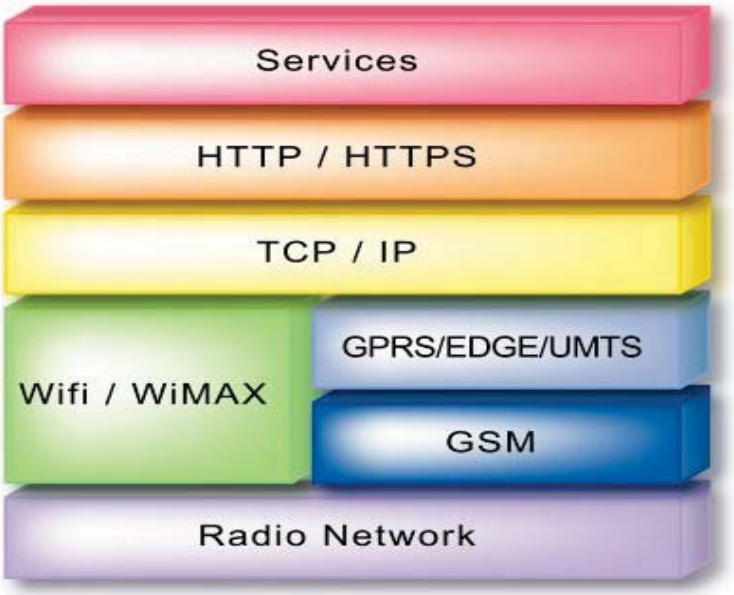


OpenSimMPLS v1.0

- Genera estadísticas detalladas de los nodos de la red.



8. Movilidad IP



Movilidad IP

- Índice
  - Introducción a la movilidad en las comunicaciones.
  - Movilidad a nivel de red.
  - Gestión de la movilidad.
  - El caso de las redes celulares. Hacia redes “All-IP”.
  - Dónde implementar la movilidad en la arquitectura TCP/IP.
  - Protocolos de movilidad IP
  - *Mobile IPv4*
  - *Mobile IPv6*

Introducción a la movilidad en las comunicaciones

- Tradicionalmente, las comunicaciones han sido fijas.
  - Nodos estacionarios.
- En los últimos años, esta situación está cambiando. Necesidades de redes de datos.
  - Los usuarios demandan redes sin cables.
  - Necesidad de comunicaciones en tiempo real.
  - Independencia del lugar, instante o medio de acceso utilizado.

Administración Avanzada de Redes TCP/IP

Introducción a la movilidad en las comunicaciones

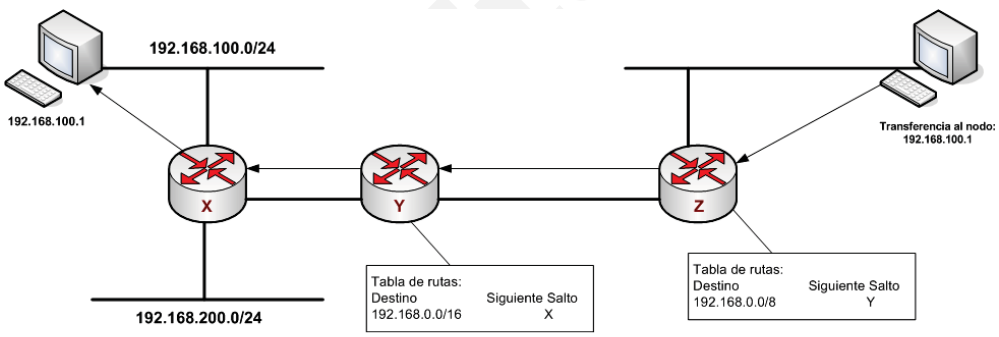
- Datos:
  - Gasto total en telefonía móvil supera a la fija. Noviembre 2005. (Fuente: Red.es)
  - Más teléfonos móviles que fijos en España. Noviembre 2006. (Fuente: Red.es)
  - Penetración de telefonía móvil en españa superó el 100% en 2006. (Fuente: Diario Cinco Días)
  - La mitad de los habitantes del mundo tendrá teléfono móvil en 2008. (Fuente: ITU – UNCTAD)

Introducción a la movilidad en las comunicaciones

- Actualmente hay que destacar dos tecnologías:
  - Arquitectura TCP/IP. Base de Internet.
  - Tecnologías inalámbricas. Base para ofrecer movilidad.
    - Movilidad: Capacidad de cambiar el punto de conexión a la red sin perder la comunicación.
    - Portabilidad: Al moverse, es necesario detener y reiniciar la comunicación.
- La convergencia de estas dos tecnologías es un reto en el campo actual de las comunicaciones.
  - Ofrecer movilidad en redes TCP/IP.

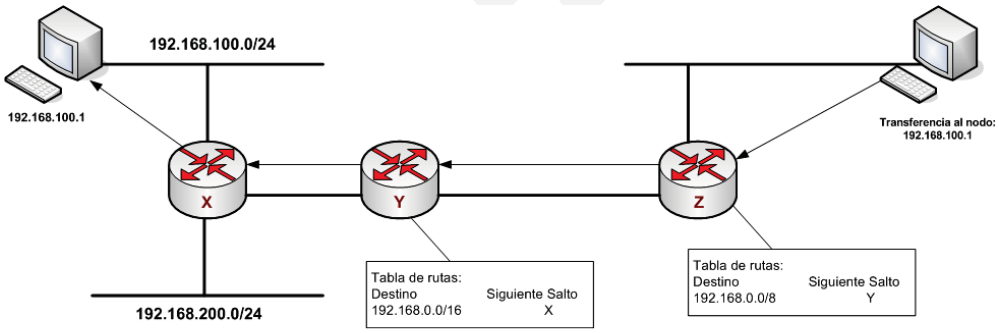
Movilidad a nivel de red

- Cualquier nodo en Internet se comunica utilizando TCP/IP. En el diseño se asumió que:
  - Los nodos eran estacionarios.
  - Cada nodo se identifica de manera única por una dirección IP.
    - Dirección formada por 2 campos: *netid* y *hostid*.



Movilidad a nivel de red

- Que todos los nodos de una red compartan un prefijo de red, hace que el encaminamiento IP escale correctamente.
- ¿Que ocurre si el nodo destino se mueve de ubicación?

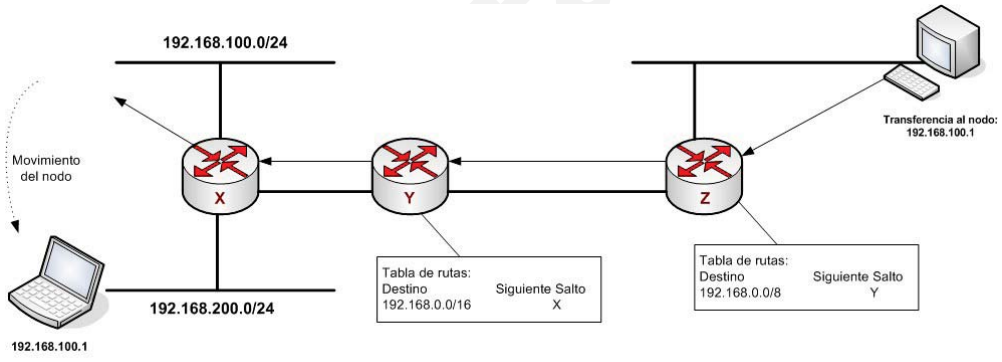


Nº 351

Administración Avanzada de Redes TCP/IP

Movilidad a nivel de red

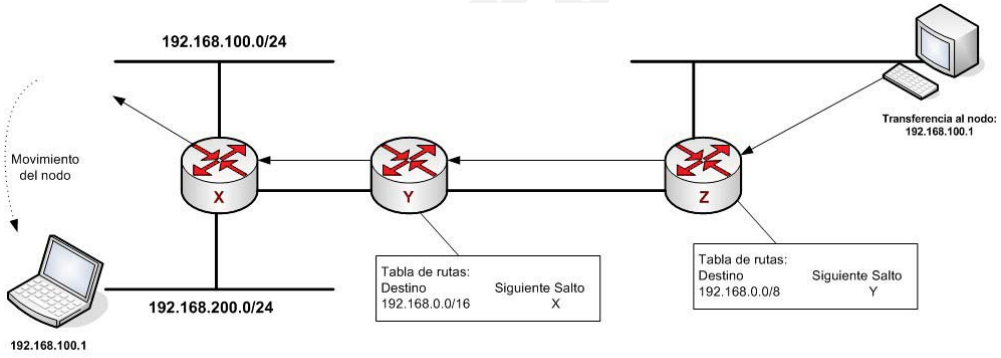
- Cuando un nodo se mueve de una red a otra, el encaminamiento tradicional no podrá remitir el paquete.
- El *netid* ahora no es válido.



Nº 352

Movilidad a nivel de red

- Para un nodo de Internet, moverse sin dejar de comunicarse significa tener que:
  - Cambiar de IP en cada movimiento. ¡Identificador TCP!
  - Propagar las rutas por la red con cada movimiento. Inabordable por problemas de escalabilidad y seguridad.

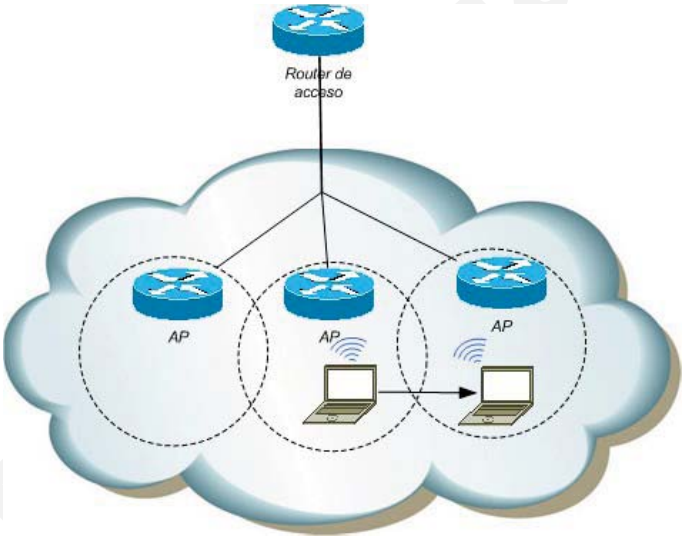


Gestión de la movilidad

- Concepto que abarca dos componentes principales:
  - Gestión de la localización (*location management*)
    - Registro o actualización de ubicación.
    - Búsqueda automática.
  - Gestión del movimiento (*handover management*)
    - Permite mantener la conexión cuando un nodo cambia su punto de conexión a la red.
- En las redes de próxima generación hay dos tipos de movimiento:
  - Intra-dominio: Movimiento entre células del mismo sistema
  - Inter-dominio: Movimiento entre distintos proveedores de servicio y posiblemente entre distintas tecnologías.

Gestión de la movilidad

- En las redes de próxima generación hay dos tipos de movimiento:
  - Intra-dominio: Movimiento entre células del mismo sistema

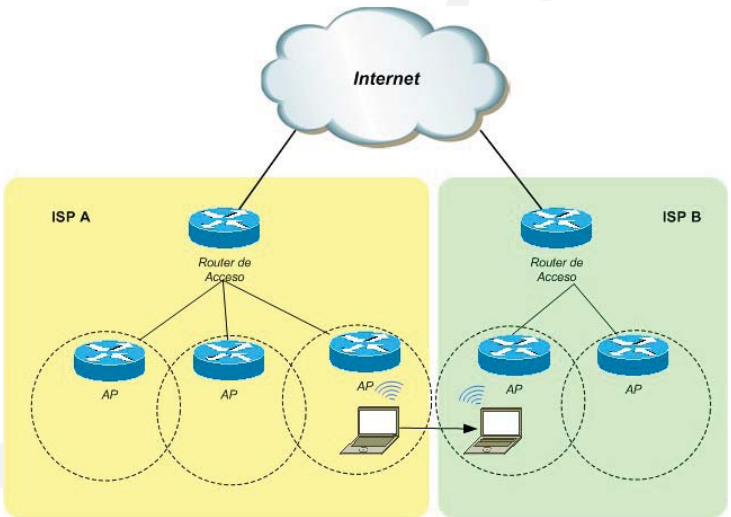


Nº 355

Administración Avanzada de Redes TCP/IP

Gestión de la movilidad

- En las redes de próxima generación hay dos tipos de movimiento:
  - Inter-dominio: Movimiento entre distintos proveedores de servicio y posiblemente entre distintas tecnologías.



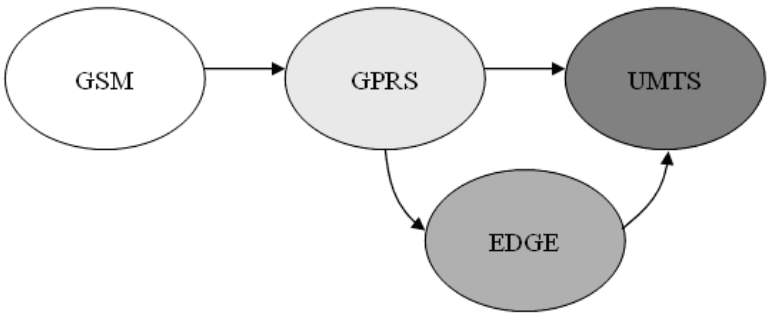
Nº 356

El caso de las redes celulares. Hacia redes "All IP"

- Las redes celulares tienen como característica inherente la movilidad.
  - Un usuario puede trasladarse de una celda a otra dentro de su red sin ver afectada la conectividad.
  - También debe disponer de conectividad desde redes de otros operadores
- Algo de historia:
  - Las redes analógicas de los años 70-80 --> 1G.
    - AMPS es el sistema más importante. Modulación FM. 1983.
  - Principio de los 80. Crecimiento de sistemas analógicos en Europa. Muchos países desarrollan sistemas propios.
  - CEPT forma un grupo para desarrollar un sistema para Europa. GSM.
  - 1990 --> GSM es el estandarte de la 2G.

El caso de las redes celulares. Hacia redes "All IP"

- Algo de historia:
  - Pronto (1994) aparecen nuevas tecnologías. GPRS (2.5G)
  - UMTS es el sistema de 3G propuesto por ETSI en 1999.
  - HSDPA (3GPP release 5) es la evolución a 3.5G.
  - 4G. Integración de tecnologías. Redes IP.



El caso de las redes celulares. Hacia redes "All IP"

- El sistema de gestión de la movilidad de GPRS y UMTS es similar
  - Basado en el protocolo GTP (*GPRS Tunnelling Protocol*)
  - La movilidad se consigue por debajo de la capa de red. Nivel de enlace.
  - La dirección de nivel 3 (nivel de red) se mantiene fija durante toda la sesión de datos.
  - Independientemente de la ubicación del terminal.
- UMTS converge hacia una red completamente IP
  - GTP puede limitar esta convergencia.
  - Mecanismos de control de la movilidad en capas superiores. En principio en IP.
- CDMA 2000 utiliza *Mobile IP* en la gestión de la movilidad.

Dónde implementar la movilidad en TCP/IP

- La movilidad puede ser implementada distintas capas de la arquitectura TCP/IP
  - Nivel 2 (enlace)
    - Buenos resultados
    - Consciente de todos los cambios en los enlaces de acceso a la red.
    - Poco impacto en nivel de aplicación (buena impresión para el usuario).
    - Problemas: Escalabilidad al no ser capaces de resolver movimientos por si mismos y difícil integración otras tecnologías.
  - Nivel superiores (4-7)
    - Muchas aplicaciones implementan algún tipo de movilidad.
    - No es completa, al no mantener sesiones al cambiar de enlace.
    - Cada aplicación debe tener su soporte de movilidad. No práctico.

Dónde implementar la movilidad en TCP/IP

- La movilidad puede ser implementada distintas capas de la arquitectura TCP/IP
  - Nivel 2 – 3 (*cross layer*)
    - Resuelve el movimiento de forma eficiente.
    - Solución de bajo retardo.
  - Nivel 3 (red - IP)
    - Lugar ideal para implementar la movilidad.
    - IP está soportado en todas las aplicaciones y enlaces (fijos e inalámbricos).
    - Movilidad transparente al nivel de transporte y superiores.
    - El usuario apenas nota el paso de conexiones fijas a inalámbricas
    - No es necesario reiniciar la conexión.

Protocolos de movilidad IP

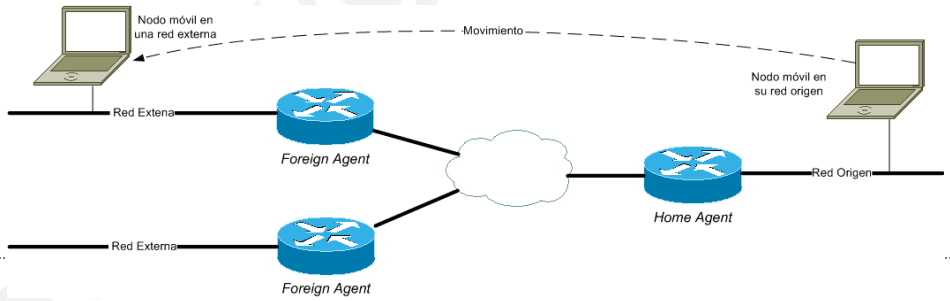
- Micro-movilidad:Movimiento de los nodos móviles entre dos subredes dentro del mismo dominio.
  - Cambios frecuentes en el punto de acceso a la red.
  - Diseñados para mantener el movimiento y proporcionar un *handover* rápido y transparente.
  - *Cellular IP*, *HAWAII*, etc.
- Macro-movilidad: Movimiento de los nodos móviles entre dos subredes de dos dominios diferentes.
  - Cooperan con los mecanismos de encaminamiento para integrar las redes fijas y móviles.
  - *Mobile IP*.

Mobile IPv4. Introduccion

- Aparece en 1996. Charles Perkins y David B. Johnson. RFC 2002.
  - Estándar “obsoleto”. Actualizado en RFC 3344.
- Surge por incapacidad de ofrecer movilidad en la actual infraestructura de Internet.
- *Mobie IP* soluciona esta situación.
  - Permite el movimiento de nodos entre redes homogéneas o heterogéneas.
- *Mobile IP* es más adecuado para macro-movilidad.

Mobile IPv4. Entidades funcionales

- Nodo móvil: *Host* que puede cambiar su punto de conexión sin cambiar su IP permanente (*Home Address*).
- *Home Agent*: *Router* de la *Home Network* del nodo móvil que envía los datagramas al nodo cuando está fuera y mantiene información de localización.
- *Foreign Agent*: *Router* de la red visitada por el nodo móvil que le proporciona servicios de encaminamiento. Extremo de salida del túnel.
- *Correspondant Node*: *Host* que se comunica con el nodo móvil.



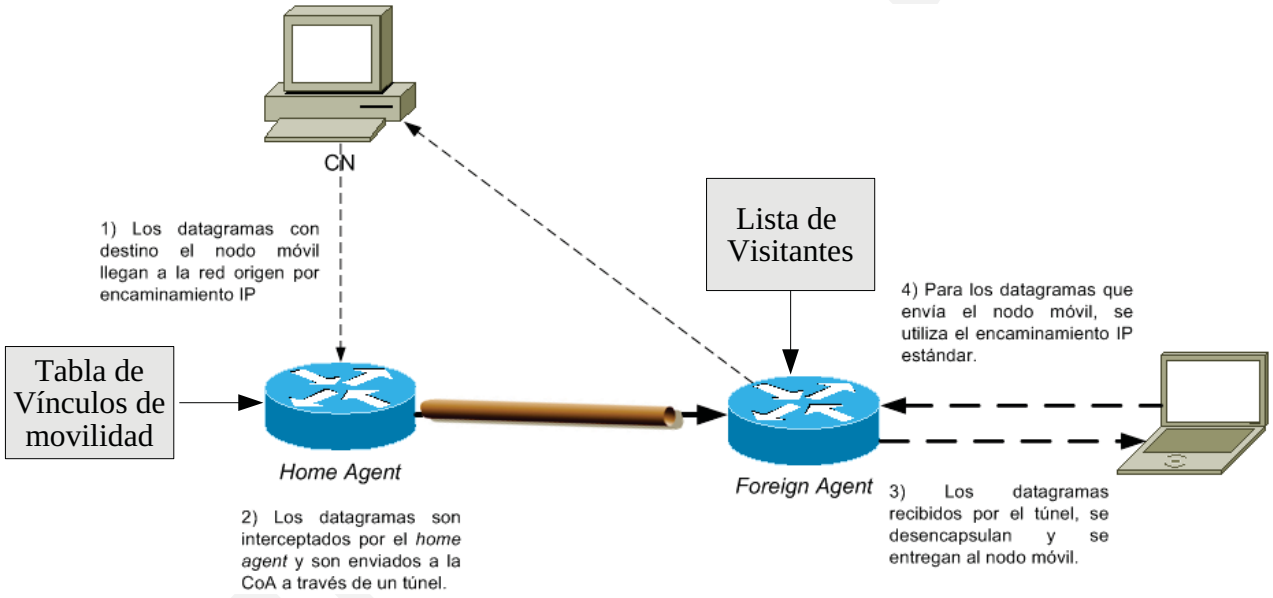
Mobile IPv4. Entidades funcionales

- *Care of-address (CoA)*: Dirección asociada al nodo cuando está fuera de su *Home Network*
  - Indica la ubicación del nodo en cada momento.
  - Punto de terminación del túnel.
  - 2 tipos:
    - *Foreign Agent CoA*: Corresponde al FA con el que el nodo móvil está registrado.
    - *Co-located CoA*: IP de la red visitada asignada temporalmente (DHCP).

Mobile IPv4. Características de movilidad de MIP

- 4 Características de cualquier protocolo de movilidad:
  - Descubrimiento de localización (Agent Advertisement/CoA asignada)
    - *Home Network*
    - *Foreign Network*
  - Detección del movimiento (*handover*)
    - Proceso de nivel 2 - 3
    - “Seguir la pista” de nivel 3 (ruta).
  - Señalización de actualización (*Reg. Request* / *Reg. Reply*)
  - (Re)Establecimiento de caminos:
    - Túnel entre la CoA y el HA.
    - Actualización tablas de encaminamiento de HA y FA.

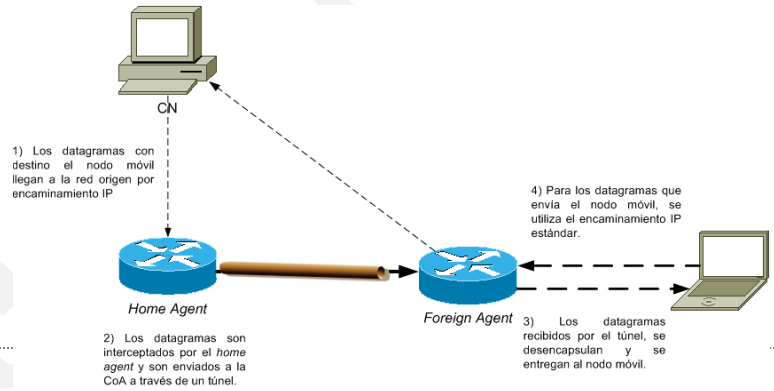
Mobile IPv4. Funcionamiento general



Administración Avanzada de Redes TCP/IP

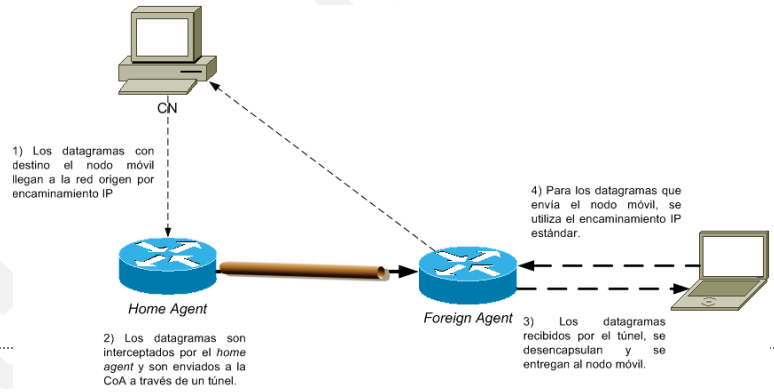
Mobile IPv4. Funcionamiento general

1. Los agentes se anuncian a través de un mensaje *Agent Advertisement*.
2. Con este mensaje, un nodo móvil determina si está en su red origen (*Home Network*) o en una red visitada (*Foreign Network*).
3. Cuando está conectado a su red origen, su funcionamiento es similar al de un nodo fijo y no utiliza las funcionalidades de *Mobile IP*.
4. Si se encuentra en una red externa, obtiene una dirección CoA. (Agent Advertisement o DHCP)



Mobile IPv4. Funcionamiento general

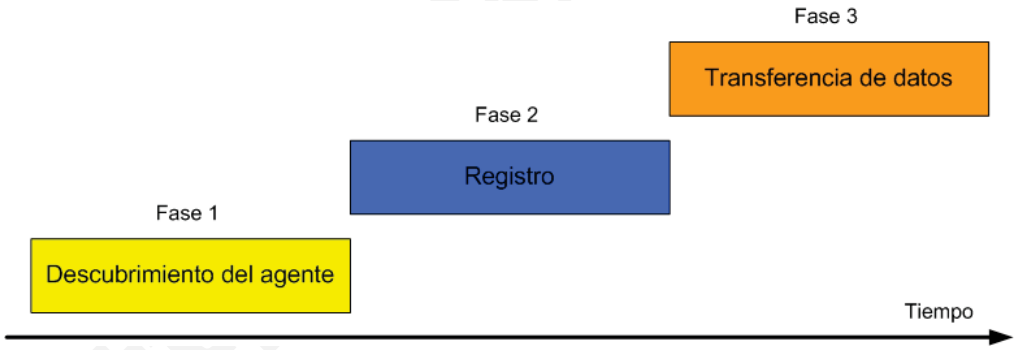
5. El nodo móvil registra su nueva dirección CoA con su HA a través de *Registration Request* y *Registration Reply*, utilizando el agente externo.
6. Los datagramas enviados a la dirección permanente del nodo, son interceptados por su HA, que los envía a la dirección CoA del nodo a través de un túnel, y finalmente son entregados al nodo móvil.
7. En el otro sentido, los datagramas enviados por el nodo móvil son entregados a su destinatario utilizando encaminamiento IP normal.



Mobile IPv4. Funcionamiento general

- El funcionamiento de Mobile IPv4 pasa por 3 fases:

1. Saber dónde se encuentra → Descubrimiento del agente
2. Informar de su ubicación actual → Registro
3. Cómo se entregan los paquetes → Transferencia de datos

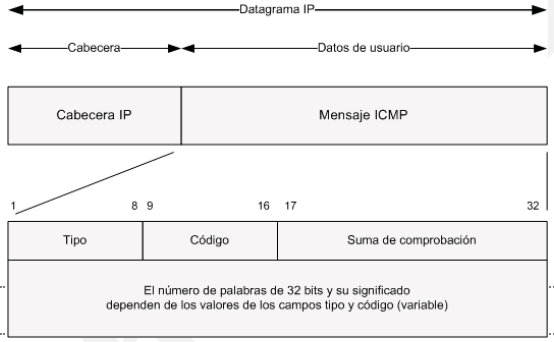


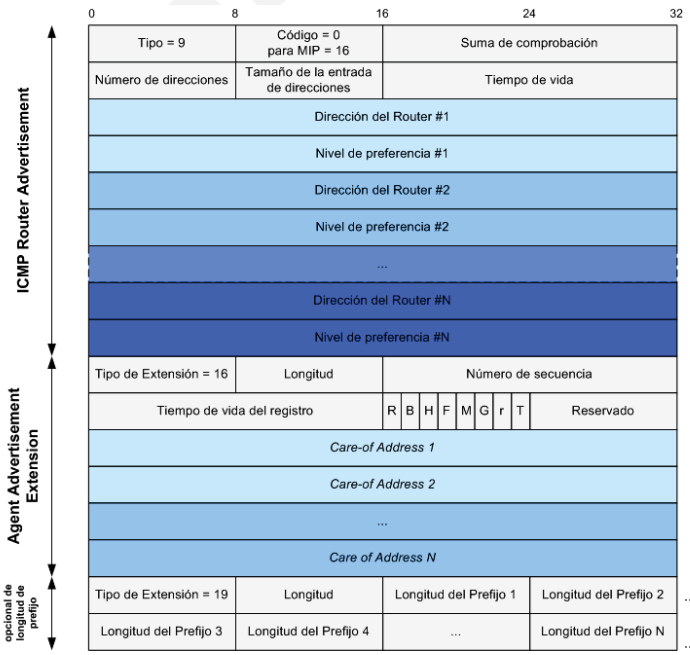
Mobile IPv4. Descubrimiento del Agente

- Intercambio de mensajes:

Mobile IPv4. Descubrimiento del Agente

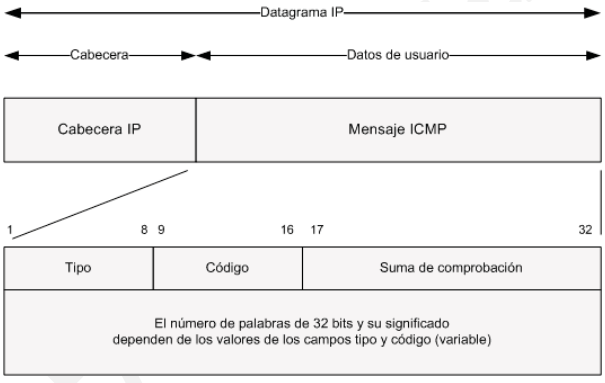
- Proceso para determinar a qué red se está conectado.
- Si ha habido movimiento.
- Permite obtener una CoA
- Mensajes ICMP
  - Agent Advertisement = ICMP Router Advertisement + Mobility Extension





Mobile IPv4. Descubrimiento del Agente

- Mensajes ICMP
  - Agent Solicitation



Mobile IPv4. Descubrimiento del Agente

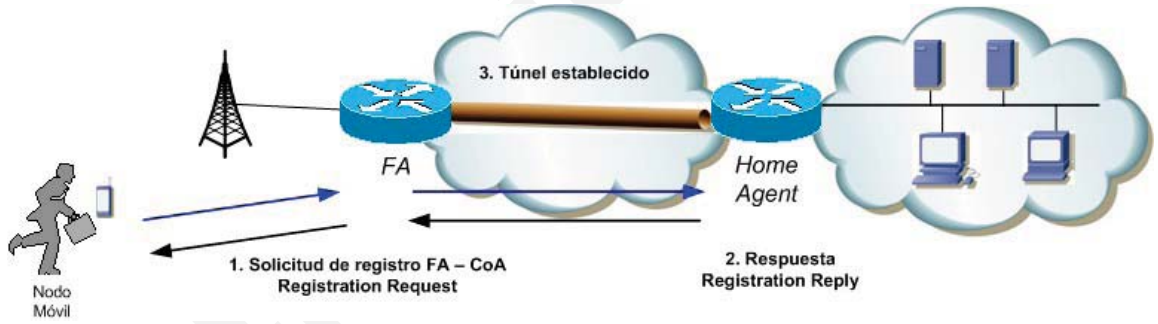
Mobile IPv4. Registro

- Proporciona un mecanismo para comunicar al HA cómo llegar hasta él.
- Crea o modifica un vínculo de movilidad en el HA, asociando la dirección permanente con su CoA.
- Se definen 2 procedimientos:
  - A través del FA, que retransmite el registro hacia el HA
  - Directamente con el HA

Administración Avanzada de Redes TCP/IP

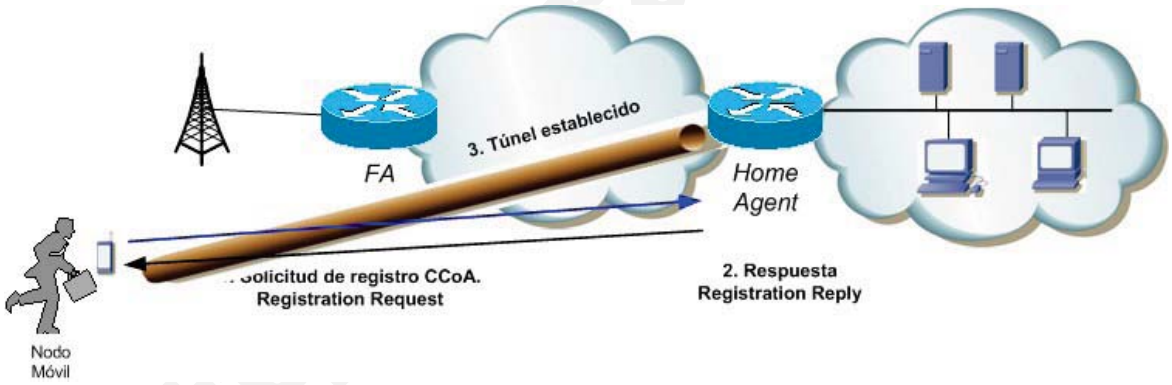
Mobile IPv4. Registro

- Registro a través del FA.
  - El nodo envía un mensaje de petición de registro al FA
  - El agente externo procesa la petición y la retransmite al HA.
  - El HA envía una respuesta al FA para admitir o denegar la petición.
  - El FA retransmite la respuesta al nodo móvil.



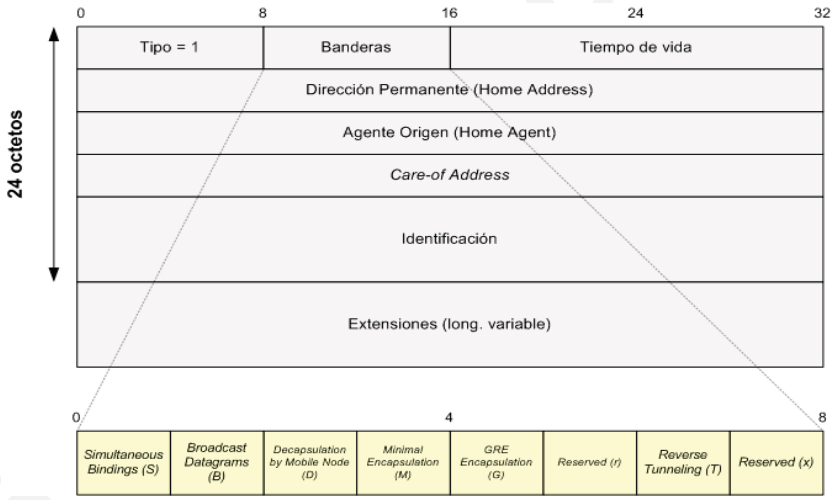
Mobile IPv4. Registro

- Directamente con el HA.
  - El nodo envía una petición de registro al HA.
  - El HA envía una respuesta al nodo aceptando o denegando la solicitud.



Mobile IPv4. *Registration Request*

- El nodo se registra con su HA utilizando *Registration Request*.
  - El HA crea o modifica el vínculo de movilidad para ese nodo
  - Se envía utilizando UDP, puerto 434.

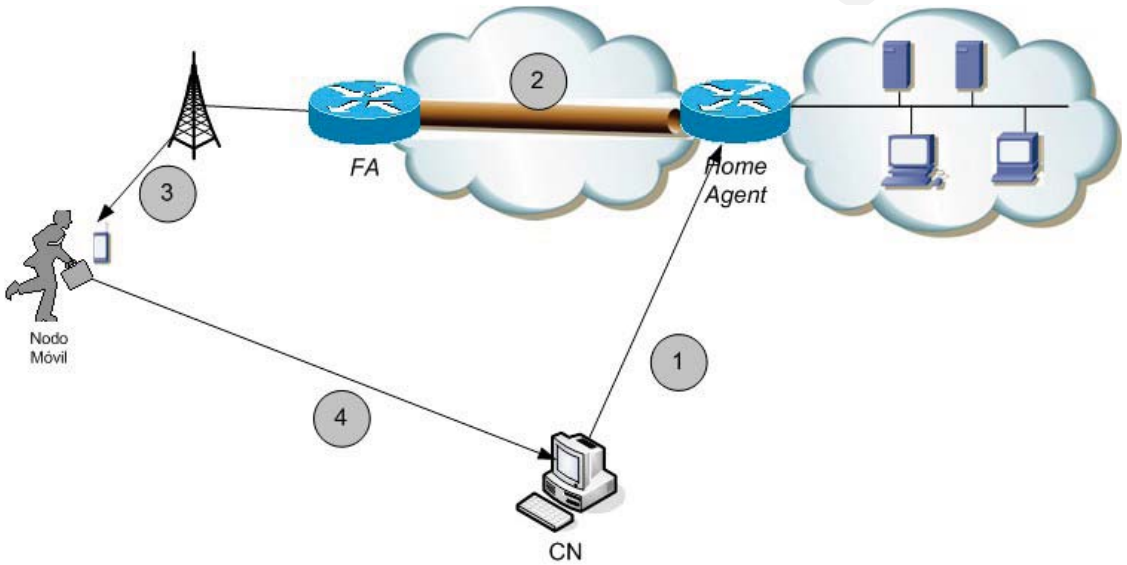


Mobile IPv4. *Registration Reply*

- Esta es la respuesta a un mensaje *Registration Request*
  - Se envía utilizando UDP, puerto 434.

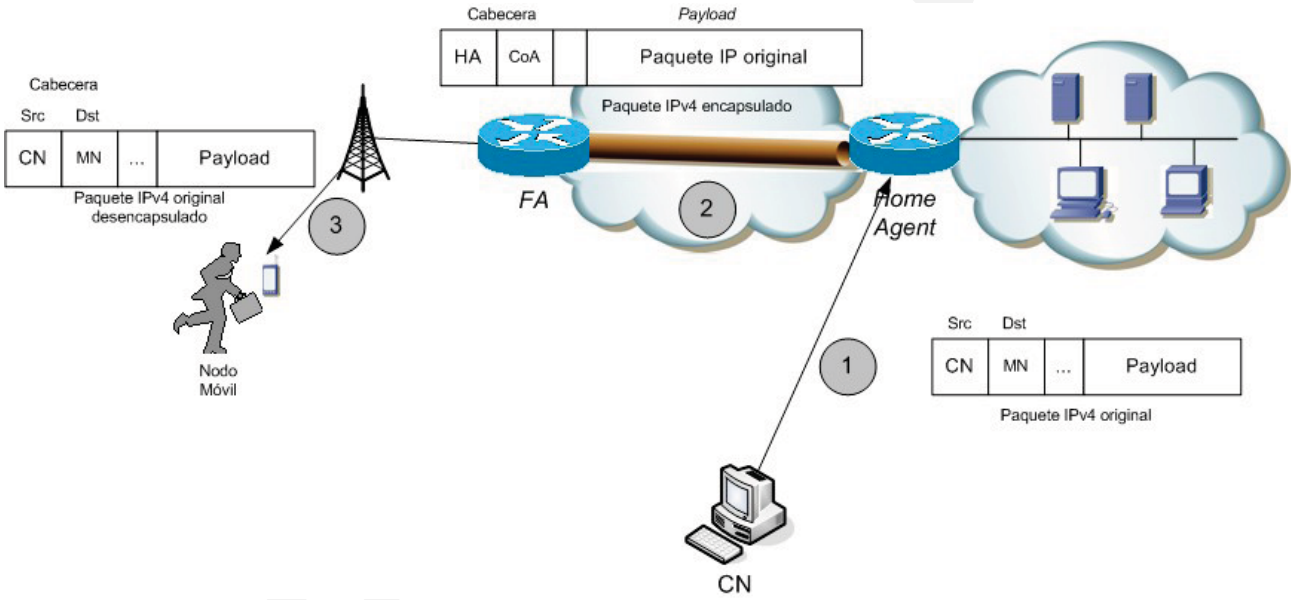
Nº 379

Mobile IPv4. Transferencia de datos



Nº 380

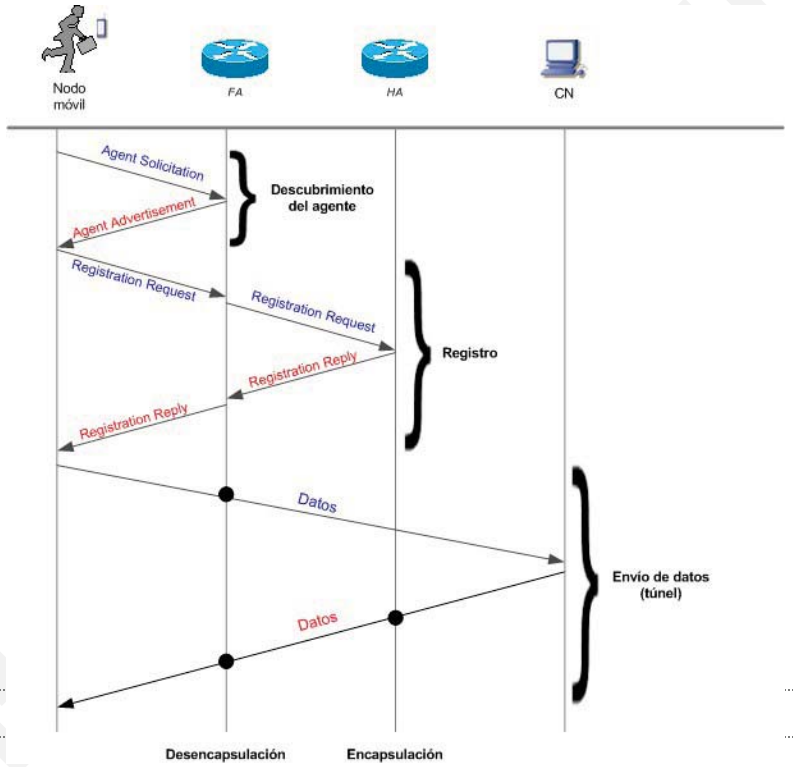
Mobile IPv4. Transferencia de datos



Nº 381

Administración Avanzada de Redes TCP/IP

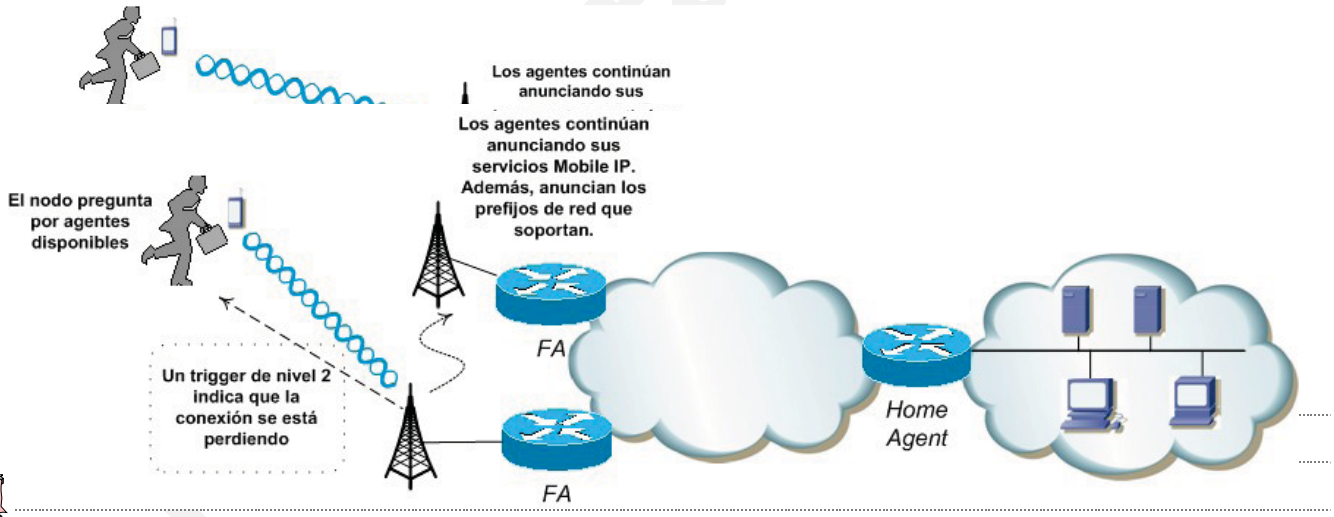
Mobile IPv4. Intercambio de Mensajes



Nº 382

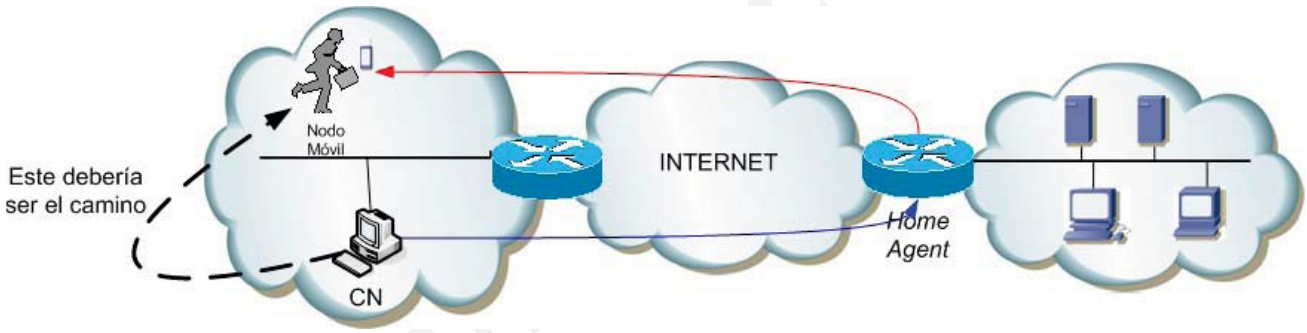
Mobile IPv4. *Handover*

- La política de *handover* gobierna el comportamiento del nodo en la detección del movimiento.
  - Reactivo
    - Algoritmo basado en el “tiempo de vida” (ICMP)
    - Algoritmo basado en prefijos de red.



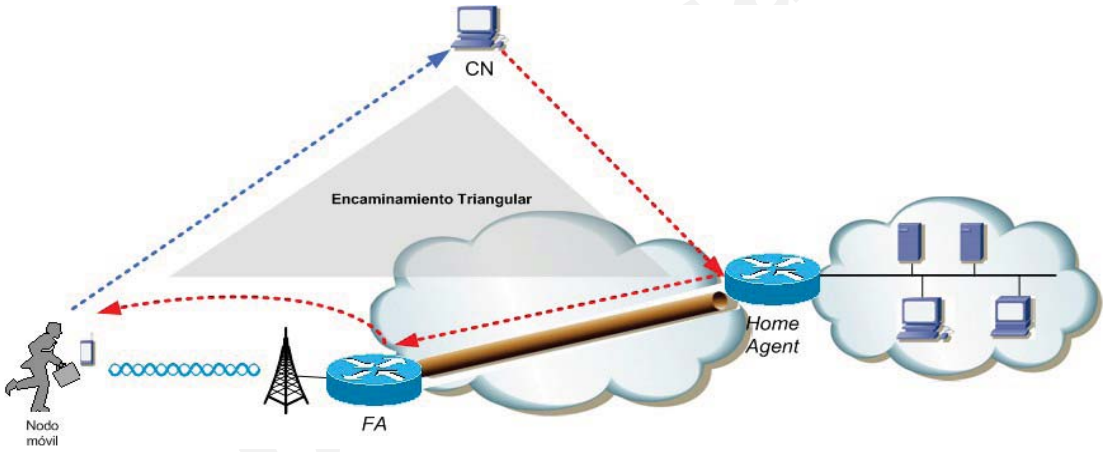
Mobile IPv4. Problemas del protocolo

- *Double Crossing*



Mobile IPv4. Problemas del protocolo

- Encaminamiento Triangular



Mobile IPv6. Introducción

- En 2004, el IETF propone *Mobile IPv6*. RFC 3775.
  - Proporciona movilidad transparente a un nodo en una red IPv6.
  - Conceptualmente, muy similar a *Mobile IPv4*.
- Beneficios:
  - El espacio de direcciones IPv6.
  - Desaparece una entidad, el *Foreign Agent*.
  - No es necesario ningún cambio para soportar MIPv6.
  - IPv6 auto-configuración simplifica la asignación de la CoA.
  - En la fase de diseño de IPv6, ya se pensaba en movilidad
    - En IPv4 era un “parche”.
    - Cabeceras de opciones, descubrimiento del vecino (para la detección del movimiento), etc.
  - El encaminamiento triangular se puede evitar con una optimización.

Mobile IPv6. Introducción

- En MIPv6, cada nodo móvil tiene dos direcciones IPv6:
  - Una dirección permanente
    - Localiza al nodo independiente de su punto de conexión a la red.
  - Una dirección temporal (CoA)
    - Auto-configuración *Stateless*
      - Recibe un *Router Advertisement* con el prefijo de la red externa y añade ese prefijo al identificador de su interfaz
    - *Stateful*
      - DHCPv6
- Caché de vínculos tanto en el HA como en los CN.

Dirección Permanente	*CoA*	*Tiempo de Vida*	*Home Agent*
3ff3:2101:0:b00::10	2001:2101:0:a00:260:97ff:fe8b:4c56	120	Si
3ff3:2101:0:b00::15	2001:2101:0:b00:a00:6aff:fe2b:137c	43	No

Mobile IPv6. Funcionamiento

- Funcionamiento Básico (túnel bidireccional)
- Optimización de la ruta

Mobile IPv6. Funcionamiento

- Dos formas posibles de comunicaciones.
  - Túnel bidireccional
    - MIPv6 utiliza un túnel IP – IP para crear una red virtual entre su CoA y el HA.
      - Para niveles superiores, el nodo siempre estará en su red.
    - No es necesario que el CN soporte MIPv6
    - No es necesario que el nodo registre su vínculo con el CN

Cabecera IPv6 (Externa)	*Cabecera IPv6 (Interna)*	*Cabecera de Transporte*	*Payload*
Dirección fuente: HAg	Dirección Fuente: CN	TCP/UDP	Datos
Dirección Destino: CoA	Dir. Destino: Dirección permanente		

Envío de tráfico por el túnel CN – Nodo móvil

Nº 389

Administración Avanzada de Redes TCP/IP

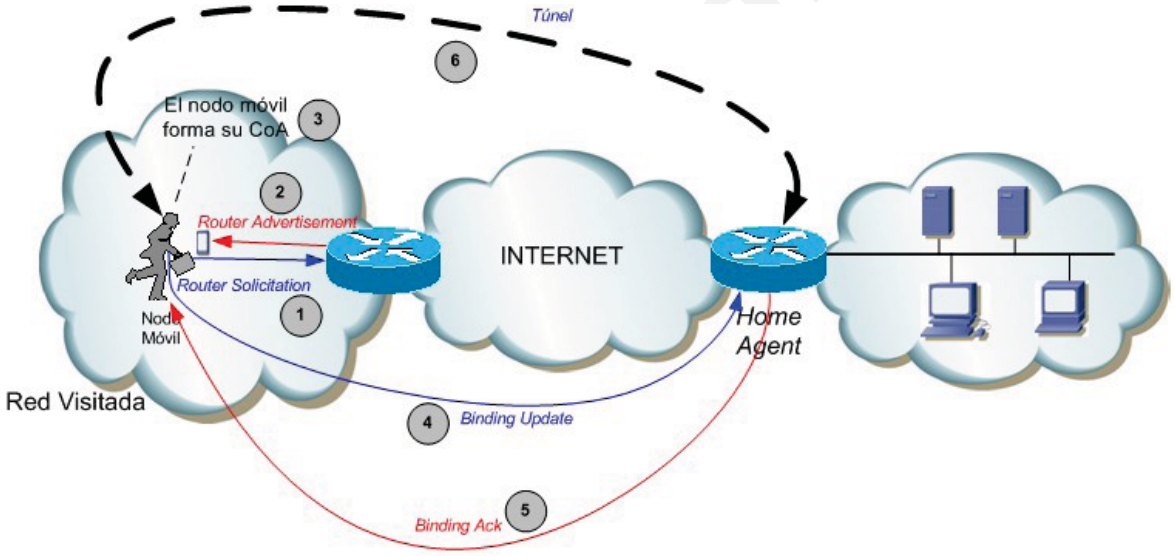
Mobile IPv6. Registro en el funcionamiento básico

- Registro con el HA:
  - El nodo móvil realiza la auto-configuración para obtener su CoA
    - Mensajes "*Router Solicitation*" y "*Router Advertisement*"
  - Registra esta CoA con su HA.
    - Usando el mensaje "*Binding Update*" con la opción de destino.
  - El HA responde con un "*Binding Acknowledgement*".
  - El túnel entre el nodo móvil y el HA estará creado.

Nº 390

Mobile IPv6. Registro en el funcionamiento básico

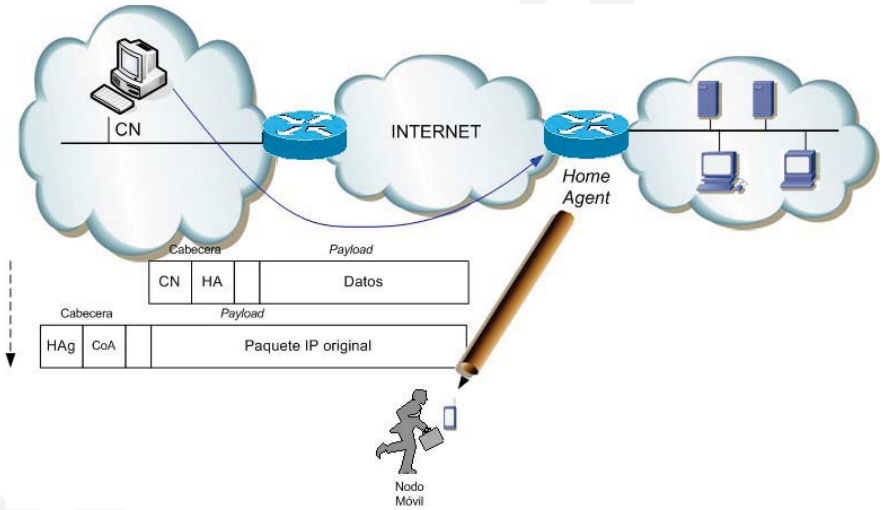
- Registro con el HA.



Nº 391

Mobile IPv6. *Routing* en el funcionamiento básico

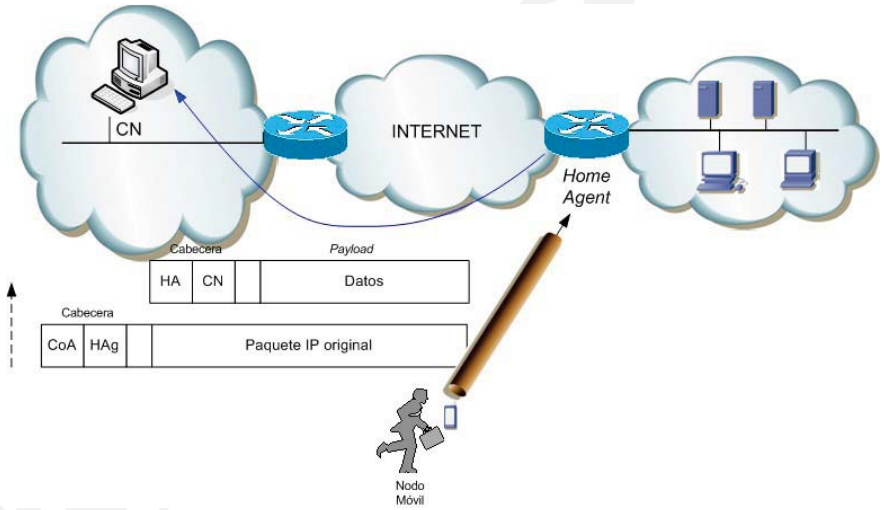
- Dos formas posibles de comunicaciones.
  - Túnel bidireccional. Camino de datos del CN al nodo móvil.



Nº 392

Mobile IPv6. *Routing* en el funcionamiento básico

- Dos formas posibles de comunicaciones.
  - Túnel bidireccional. Camino de datos del nodo móvil al CN.



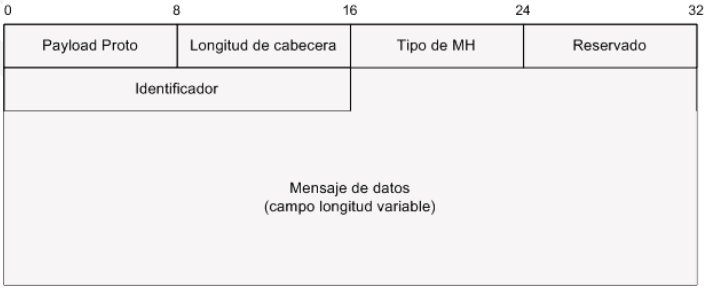
Mobile IPv6. Funcionamiento

- Dos formas posibles de comunicaciones.
  - *Route Optimization*
    - Los paquetes desde el CN se encaminan directamente a la CoA.
    - Se elimina la congestión en el HA y en su enlace.
    - Mecanismo de seguridad. Protocolo RR (*Return Routability*)
    - Envío de datos
      - Del nodo móvil al CN se usa HAO (*Home Address Option*).
        - » Necesario traducir la dirección fuente: La CoA es reemplazada por la permanente en el campo fuente.
      - Del CN al nodo móvil utiliza una nueva cabecera IPv6 de encaminamiento llamada de tipo 2.
        - » Necesario traducir la dirección de destino. La CoA es reemplazada por la dirección permanente en el campo destino

Mobile IPv6. Cabecera de movilidad

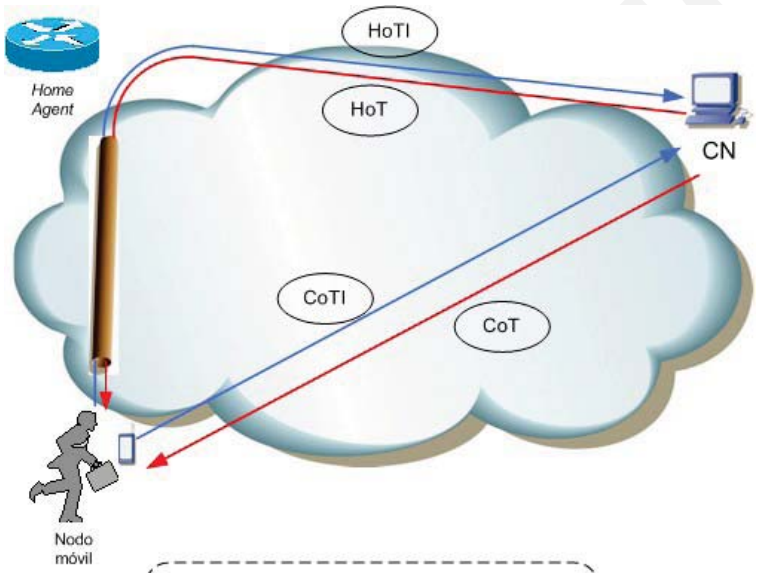
- *Mobile IPv6* define una nueva cabecera IPv6. Cabecera de movilidad.
  - Utilizada en los mensajes relacionados con la creación y gestión de vínculos
- Mensajes soportados por la cabecera de movilidad.
  - *Home Test Init*
  - *Home Test*
  - *Care-of Test Init*
  - *Care-of Test*
  - *Binding Update*
  - *Binding Acknowledgement*
  - *Binding Refresh Request*
  - *Binding Error*

Return Routability



Registro

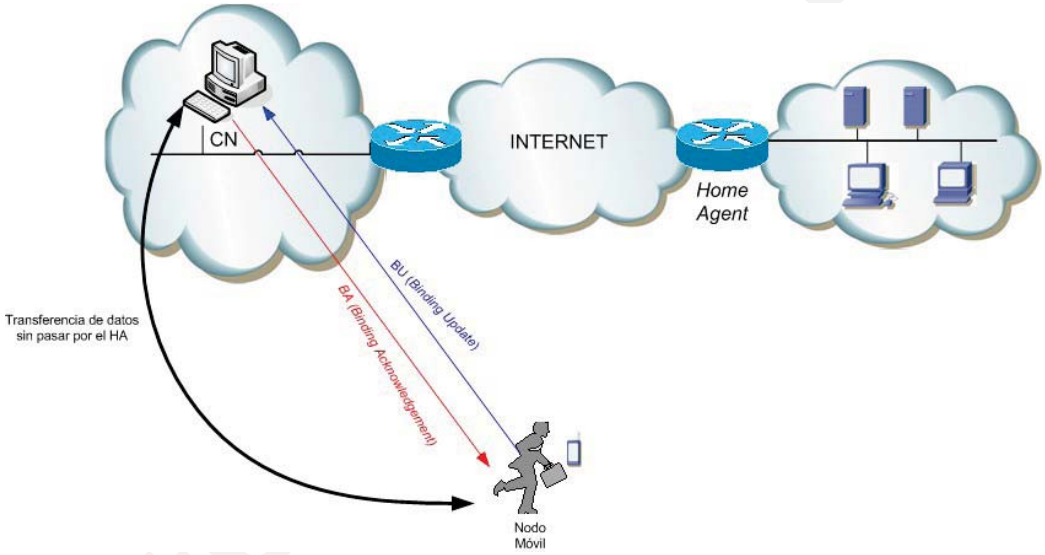
Mobile IPv6. *Return Routability*



HoTI. Solicitud para una parte de la clave
CoTI. Solicitud para otra parte de la clave
HoT. Token para la dirección permanente
CoT. Token para la dirección CoA

Los nodos móviles generan tokens claves en los CN después de recibir ambas respuestas

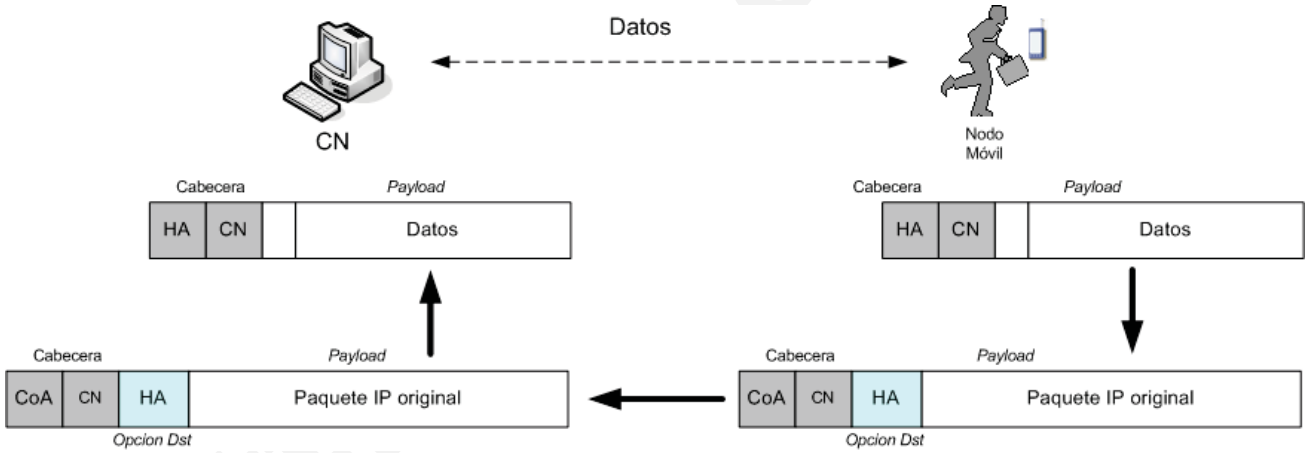
Mobile IPv6. Gestión de vínculos



Nº 397

Mobile IPv6. Funcionamiento

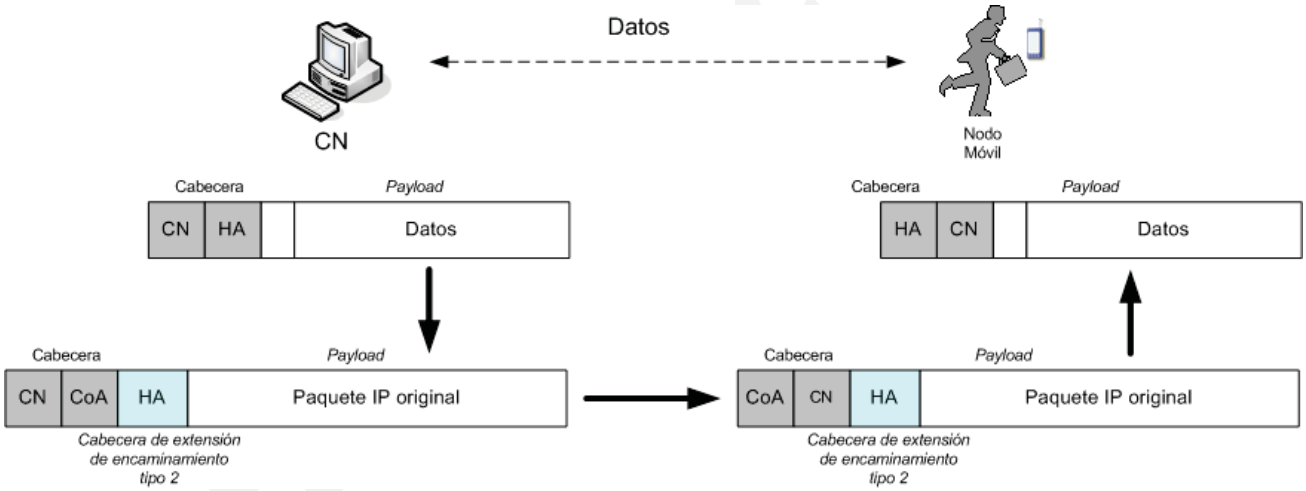
- Dos formas posibles de comunicaciones.
  - *Route Optimization*
    - MN ⟶ CN



Nº 398

Mobile IPv6. Funcionamiento

- Dos formas posibles de comunicaciones.
  - *Route Optimization*
    - CN ⟶ MN

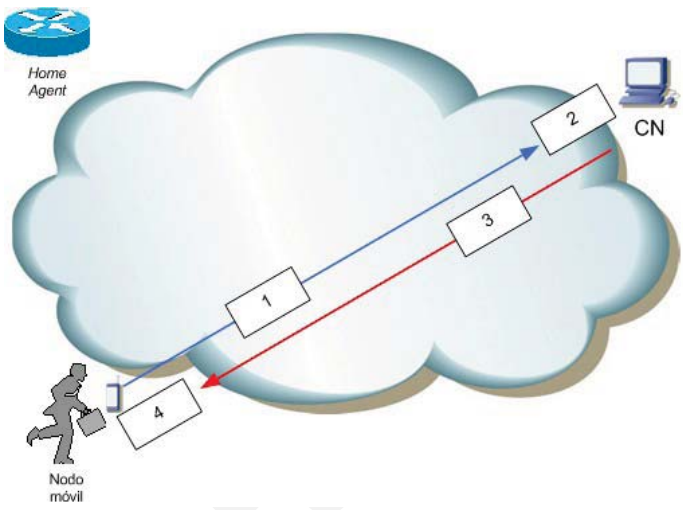


Nº 399

Administración Avanzada de Redes TCP/IP

Mobile IPv6. Funcionamiento

- Dos formas posibles de comunicaciones.
  - *Route Optimization*

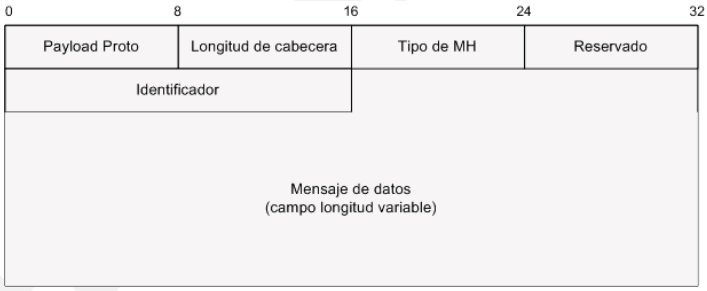


Número de paquete	Dirección IP Fuente	Dirección IP Destino	Cabecera de routing tipo 2	Opción Home Address
1	Care-of Address	Dirección CN	Ninguna	Presente
2	Dirección permanente	Dirección CN	Ninguna	Presente
3	Dirección CN	Care-of Address	Dirección permanente	Ninguna
4	Dirección CN	Dirección permanente	Dirección permanente	Ninguna

Nº 400

Mobile IPv6. Nuevas cabeceras de extensión

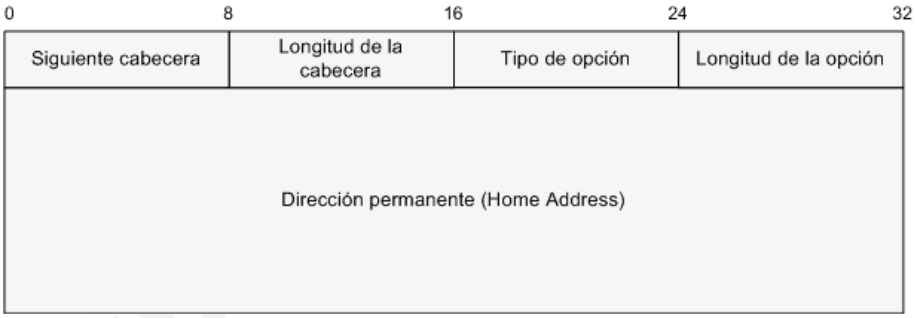
- A la cabecera IPv6:
  - Crea una nueva cabecera de extensión – *Mobility Header*
  - Añade un tipo de cabecera de encaminamiento
  - Añade una nueva opción de destino.
- Cabecera de movilidad
  - Mensajes de creación y gestión de vínculos.



Administración Avanzada de Redes TCP/IP

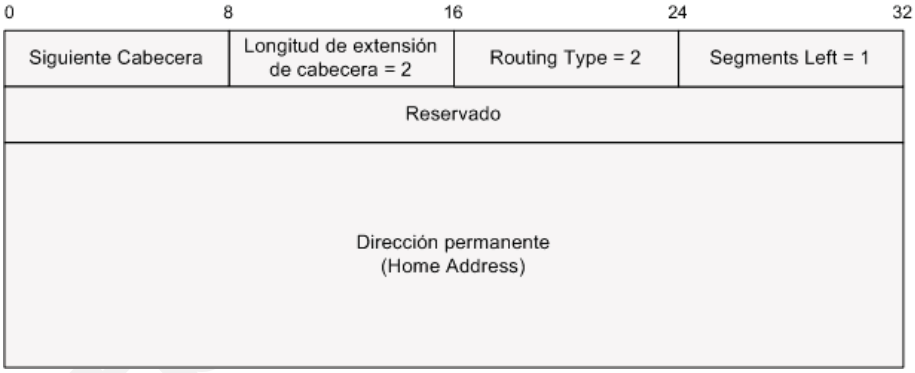
Mobile IPv6. Nuevas cabeceras de extensión

- Cabecera de opción de destino
  - Transporta la HA
  - Paquetes enviados por un nodo móvil, para informar al receptor de su dirección permanente



Mobile IPv6. Nuevas cabeceras de extensión

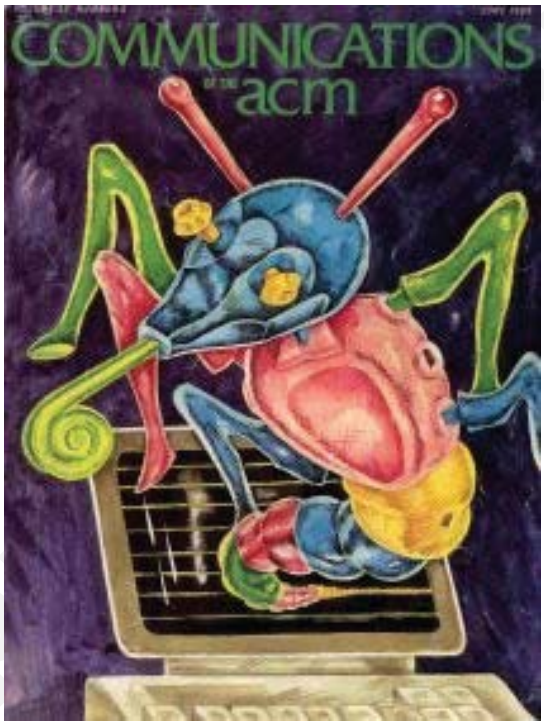
- Cabecera de encaminamiento Tipo 2
  - Variante de cabecera de encaminamiento para permitir a los paquetes ser encaminados del CN a la CoA directamente.



Mobile IPv6. Simulación

OMNET++

9. Seguridad en redes IP



9) Seguridad en redes IP

Objetivos

- Introducir CSI (Comunicaciones y Seguridad de la Información).
- Revisar la seguridad en IPv4.
- Analizar las posibilidades de seguridad nativa en IPv6.
- Practicar con herramientas para mitigar los riesgos.

9) CSI (Comunicaciones y Seguridad de la Información)

- Debilidades seguridad:
  - Sistemas operativos.
  - Protocolos redes y comunicaciones.
  - y usuarios confiados.

- Suma atención, cuidado y seguimiento diario.

- Soluciones:
  - Sistemas operativos reforzados (nivel C2).
  - Comunicaciones seguras (IPv6, cifrado, firewalls...).
  - Usuarios concienciados (formación, inversión).

Administración Avanzada de Redes TCP/IP

9) CSI (Comunicaciones y Seguridad de la Información)

Seguridad informática: protege ordenador y lo relacionado con él (acceso físico, cableados, periferia, etc.). ***Seguridad de la información***.

- Intenciones de los accesos no autorizados:
  - Obtención de información valiosa.
  - Destruir información.
  - Pura curiosidad.
  - Demostrar que se ha conseguido franquear las barreras.
- Otros peligros menos espectaculares pero más habituales:
  - Errores humanos.
  - Inexistencia de ***política de seguridad***.
  - Contraseñas compartidas.
  - Desconocimiento....

9) CSI (Comunicaciones y Seguridad de la Información)

• Amenaza: en un entorno informático es cualquier elemento que compromete el sistema.

• Las amenazas pueden analizarse: antes, durante o después del ataque. Estos mecanismos conforman políticas que garantizan la seguridad del sistema informático:

• La prevención (antes): como mecanismo que aumenta la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Ej. Cifrado de la info. antes de transmitirla.

• La detección (durante): Mecanismo orientado a revelar violaciones a la seguridad. Suelen ser programas de auditoría.

Administración Avanzada de Redes TCP/IP

9) CSI (Comunicaciones y Seguridad de la Información)

• La recuperación (después) mecanismos que se aplican, cuando la violación del sistema ya se ha detectado para restaurarlo a su funcionamiento normal (recuperación desde copias de seguridad).

• Preguntas que debe resolver un Administrador de Redes ante un problema de seguridad:

• ¿Cuánto tardará la amenaza en superar la “solución planteada”?
• ¿Cómo se detecta e identifica a tiempo la amenaza?
• ¿Cómo se neutraliza?

9) CSI (Comunicaciones y Seguridad de la Información)

• Riesgo: la proximidad o posibilidad de daño sobre un bien. Actos naturales, errores u omisiones humanas y actos intencionados. Cada riesgo debe atacarse:

  • Minimizando la posibilidad de su ocurrencia.
  • Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
  • Diseño de métodos para la más rápida recuperación de los daños experimentados.
  • Corrección de las medidas de seguridad en función de la experiencia recogida.

Administración Avanzada de Redes TCP/IP

9) CSI (Comunicaciones y Seguridad de la Información)

• Para garantizar que una red sea fiable se debe conocer:
  - Qué se quiere proteger.
  - De quién se quiere proteger.
  - Cómo se puede lograr técnica y legalmente.
  - Formular estrategias de seguridad para disminuir o anular riesgos.

• Conocer y comprender la seguridad ayuda a llevar a cabo análisis sobre:
  - Los riesgos, vulnerabilidades, amenazas y contramedidas.
  - Evaluar las ventajas o desventajas de la situación.
  - Decidir medidas técnicas y tácticas metodológicas, físicas e informáticas en base a las necesidades de seguridad.

9) CSI (Comunicaciones y Seguridad de la Información)

• De quién hay que protegerse:Intruso o atacante es cualquier persona que accede (o lo intenta) sin autorización a un sistema ajeno, sea de forma intencionada o no. Tipos de intrusos:

- Clase A: el 80%. Son la base, los nuevos intrusos que bajan programas de Internet y “juegan” para probar.
- Clase B: 12 % y los más peligrosos. Saben compilar programas pero no programar. Prueban programas, testean vulnerabilidades y acceden por ellas.
- Clase C: el 5% que sabe, conoce y define sus objetivos. Buscan todos los accesos remotos e intentar acceder.
- Clase D: 3 % restante que cuando entran a determinados sistemas saben lo que buscan.

Administración Avanzada de Redes TCP/IP

9) CSI (Comunicaciones y Seguridad de la Información)

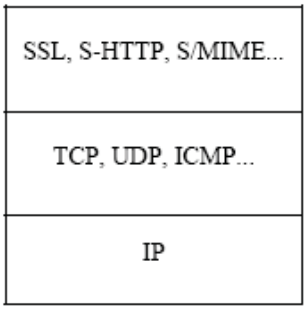
• Qué hay que proteger:

- El hardware.
- El software (SO, aplicaciones y utilidades).
- Los datos o conjunto de informaciones lógicas que maneja el software y el hardware: archivos, documentos, bases de datos, etc . Son los más importantes.
- Fungibles: toner, cintas magnéticas, papel, discos, CDs, etc.

• Importante entender que no existe el 100% de seguridad esperado o deseable.

9) Seguridad en IPv4

IPv4: no contempla la seguridad en su diseño original, por lo que fue necesario incluirla en la capa de Aplicación.



Protocolos de seguridad en capas superiores

- SSH (Secure SHell)
- SSL (Secure Socket Layer)
- S-HTTP (Secure Hypertext Transfer Protocol)
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- SET (Secure Electronic Transaction)
- Firma digital (Autentificación, integridad y no revocación)

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv4

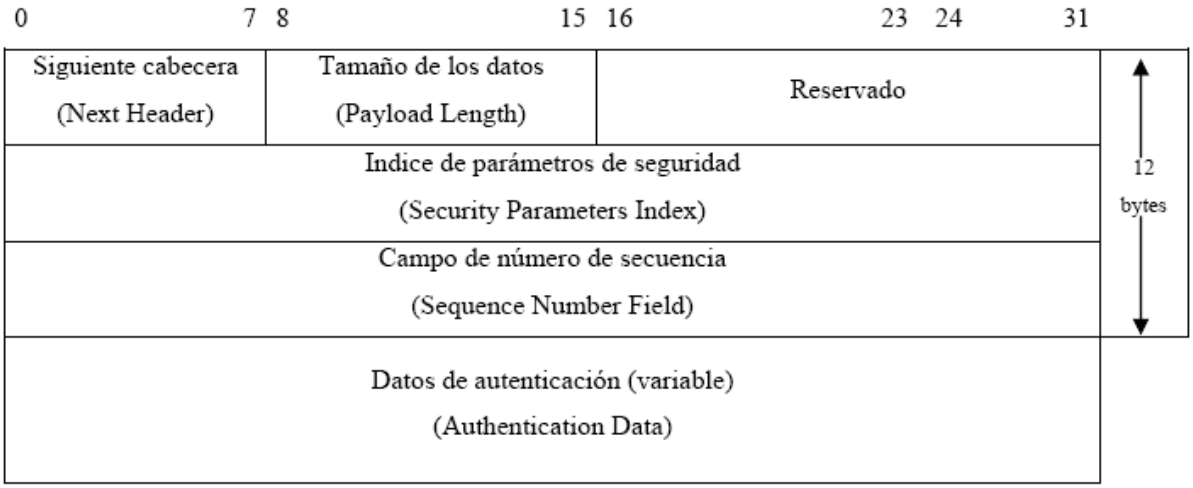
IPv4: es robusto y fiable. Permite la independencia de los protocolos de capas superiores.

Necesidades de revisión:

- Direccionamiento insuficiente.
- Sobrecarga routers.
- Inseguridad.

9) Seguridad en IPv6

Cabecera de autentificación: una de las novedades más importantes de IPv6. Debe estar situada entre la cabecera y los datos. La presencia de esta cabecera no modifica el comportamiento del resto protocolos superiores. Esta cabecera tan sólo proporciona una seguridad implícita del origen del datagrama, así, los protocolos de capas superiores deben rechazar los paquetes que no estén adecuadamente autentificados.



Nº 417

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

Cabecera de autentificación: una de las novedades más importantes de IPv6. Debe estar situada entre la cabecera y los datos. La presencia de esta cabecera no modifica el comportamiento del resto protocolos superiores. Esta cabecera tan sólo proporciona una seguridad implícita del origen del datagrama, así, los protocolos de capas superiores deben rechazar los paquetes que no estén adecuadamente autentificados.

Cabecera IPv6 (siguiente = **TCP**)	Cabecera de autenticación (Authentication Header)	Cabecera TCP + Datos	
Cabecera IPv6 (siguiente = **routing**)	Cabecera Routing	Cabecera de autenticación (Authentication Header)	Cabecera TCP + Datos
Cabecera IPv6 (siguiente = **routing**)	Cabecera de autenticación (Authentication Header)	Opciones al destino (End-to-end options)	Cabecera TCP + Datos

Situación de la cabecera de autentificación

Nº 418

9) Seguridad en IPv6

IPSec son un conjunto de especificaciones para garantizar la seguridad como parte Implícita de las nuevas especificaciones de los protocolos.

Para evitar duplicidades y asegurar un sistema seguro y auténtico en todas las capas se optó por incluir las especificaciones en el nivel más bajo de la pila de protocolos, IPv6.

RFCs: 2104, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2410, 2411, 2412, 2451

La seguridad en IPSec se proporciona mediante dos aspecto de seguridad:
- Cabecera de autentificación (authentication Header AH): cabecera encargada de proporcionar autenticidad a los datos que se reciben. Los datagramas provienen del origen especificado (se garantiza la autenticidad de los datos, no repudio) y no han sido modificados.
- Cifrado de seguridad (Encrypted Security Payload, ESP) para garantizar que sólo el destinatario legítimo del datagrama pueda descifrar su contenido.

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

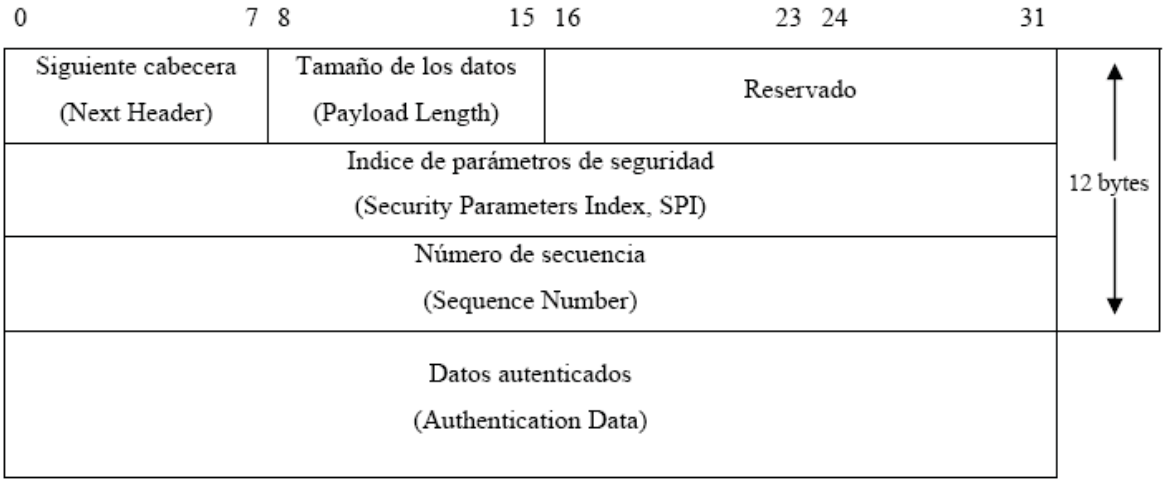
IPSec:

-La autenticidad y el cifrado de datos requiere que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como tiempo de validez de la clave) que diferencia una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (SA) que permite unir la autenticidad y la seguridad en IPSec.

La cabecera de autentificación (AH): Cabecera específica de IPv6 que se designa con el número 51. Se suele situar justo antes de los datos de forma que los proteja de posibles atacantes, aunque puede incluirse antes de otras cabeceras para asegurar que las opciones que acompañan al datagrama son correctas.
Así, la presencia de una AH no modifica el funcionamiento de protocolos superiores ni el de los routers intermedios que sólo encaminan el datagrama al destino.

9) Seguridad en IPv6

AH:



Estructura de la cabecera de autentificación

Nº 421

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

AH:
El tamaño de datos especifica la longitud de los datos en palabras de 32 bits.

El índice de parámetros de seguridad (SPI) es un número de 32 bits que permite identificar un gran número de conexiones de IPSec activas en un mismo ordenador.

El número de secuencia identifica el número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entregas de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas.

Datos autentificados se obtienen realizando operaciones (dependendiendo del algoritmo de cifrado elegido) entre algunos campos de la Cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.
El principal problema de autentificar un datagrama es que algunos campos son modificados por los routers intermedios por lo que el datagrama va cambiando en su camino por internet. Suele usarse MD5 que calcula un checksum de 128 bits.

Nº 422

9) Seguridad en IPv6

Cabecera de cifrado de seguridad (ESP, Encrypted Security Payload):

La AH no modifica los datos que transporta, circulan en texto plano, y sólo añaden autenticidad (al origen y contenido). Los datos pueden ser interceptados y visualizados y puede ser útil (BOE, periódicos digitales, etc), y no interesa cifrarlos.

Cuando interese confidencialidad (saldos bancarios, etc) se debe usar la cabecera ESP.

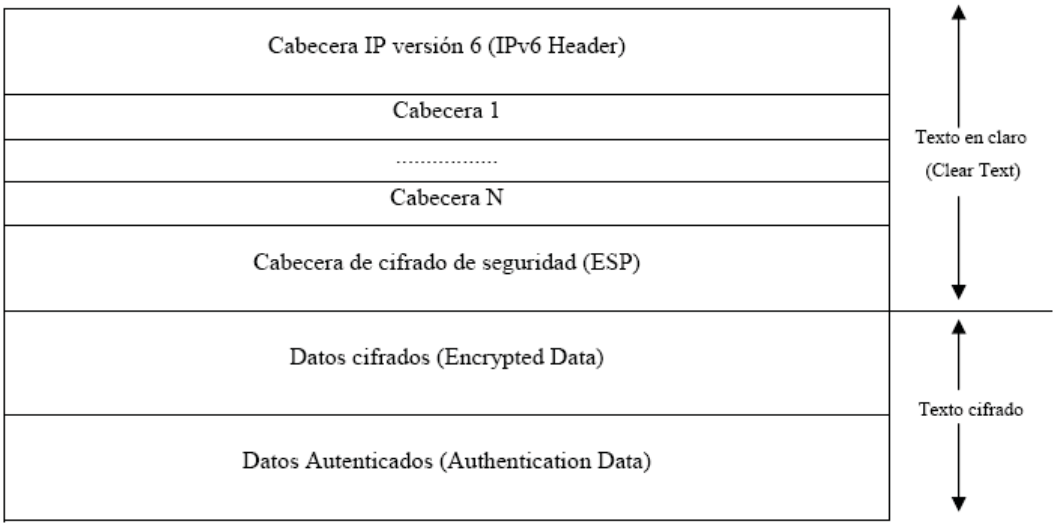
Esta cabecera es siempre la última en el sistema de cabeceras en cadena. Esto es debido a que a partir de ello todos los datos vienen cifrados, con los que los routers intermedios no podrían procesar las cabeceras posteriores.

Nº 423

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

Cabecera de cifrado de seguridad (ESP, Encrypted Security Payload):

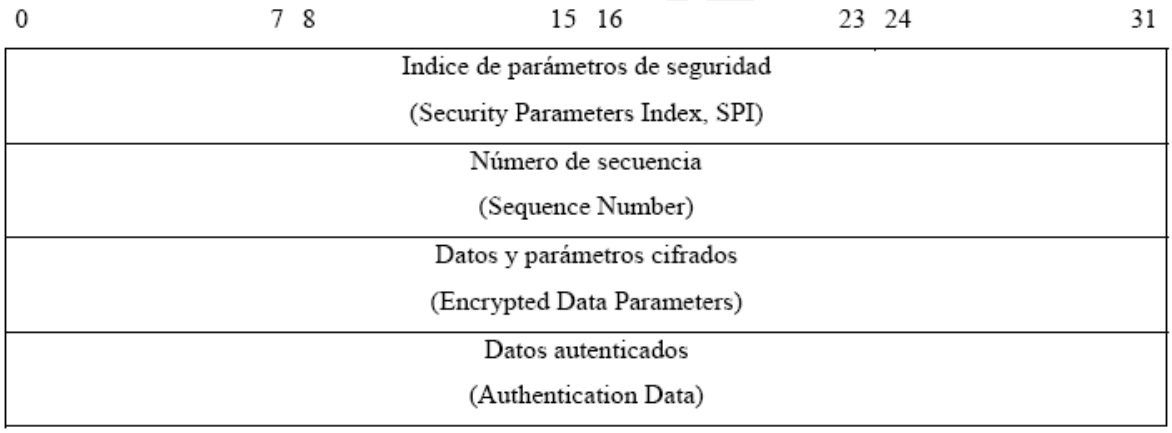


Situación de la cabecera de cifrado de seguridad (ESP)

Nº 424

9) Seguridad en IPv6

Cabecera de cifrado de seguridad (ESP, Encrypted Security Payload):



Estructura de la cabecera de cifrado de seguridad (ESP)

Nº 425

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

Cabecera de cifrado de seguridad (ESP, Encrypted Security Payload):

Como en las AH, el algoritmo a usar se negocia con el receptor antes de enviar un datagrama cifrado. Se propone DES-CBC.

Al contrario de AH, no es necesario especificar el tamaño de los datos cifrdos, ya que a partir de la cabecera de cifrado hasta el final del datagrama todo está cifrado.

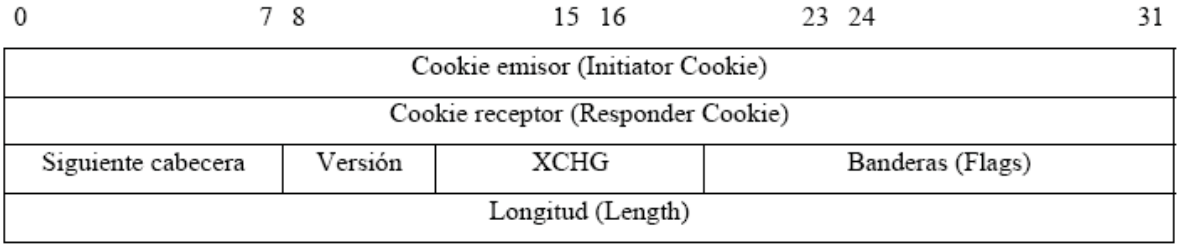
El índice de parámetros de seguridad (SPI) y el número de secuencia tienen el mismo significado que en AH.
Los datos autentificados aseguran que el texto cifrado no ha sido modificado usando un algoritmo de hash.
Como tanto AH como ESP pueden ser usadas independientemente, se recomienda que si se necesita tanto la autenticidad como la privacidad, se incluya la cabecera de cifrado tras la de autentificación, para así autentificar todos los datos cifrados.

Nº 426

9) Seguridad en IPv6

Protocolo ISAKMP (Internet Security Association Key Management Protocol):

Propuesto para el intercambio de claves y parámetros de seguridad en IPSec como antes lo fueron SKIP, Phouturis, Oakley, etc.



Formato de la cabecera ISAKMP

Nº 427

Administración Avanzada de Redes TCP/IP

9) Seguridad en IPv6

- La extensión de cabeceras de IPv6:
  - Aporta seguridad extremo-a-extremo:
    - Servicios IPsec entre pares de nodos.
    - Autentificación separada del cifrado.

  - Cabecera de Autentificación (AH):
    - Paquete completo.
    - Aporta integradad de datos y autentificación.
    - Mitiga las réplicas.

  - Cabecera de Encapsulation Security Payload (ESP):
    - Encapsula el campo de datos (transporte) y paquetes (túneles).
    - Aporta autentificación e integridad de datos y/o confidencialidad.
    - Mitiga las réplicas.
    - Limita el sniffing (con confidencialidad activada).

Nº 428

9) Seguridad en IPv6

- La seguridad nativa en IPv6 tiene limitaciones:
  - El algoritmo de cifrado DES es débil.
  - PKI no está completamente estandarizado.
  - Gestión manual de claves, al menos inicialmente,:
    - Carece de mecanismos de distribución de claves global.
  - IKE debe ser mejorado frente a DoS.

- IPsec no es la respuesta a todos los problemas de seguridad en IPv6.
- IPv6 necesita mejoras de seguridad adicionales.
- La movilidad introduce cambios en la seguridad.
- Las infraestructuras de pilas duales requieren reglas de seguridad IPv4 e IPv6.
- Las autoridades de seguridad (certificados) deben gestionar tanto IPv4 como IPv6.

9) Herramientas de hacking para IPv6

Sniffers/captura de paquetes:

- Snort
- TCPdump
- Sun Solaris Snoop
- COLD
- Ethereal
- Analyzer
- Windump
- WinPcap
- NetPeek
- Sniffer Pro

Scanners:

- IPv6 Security Scanner
- Halfscan6
- Nmap
- Strobe
- Netcat

9) Herramientas de hacking para IPv6

Herramientas DoS:

- 6tunneldos
- 4to6ddos
- Imps6-tools

Packet forgers:

- SenIP
- Packit
- Spak6

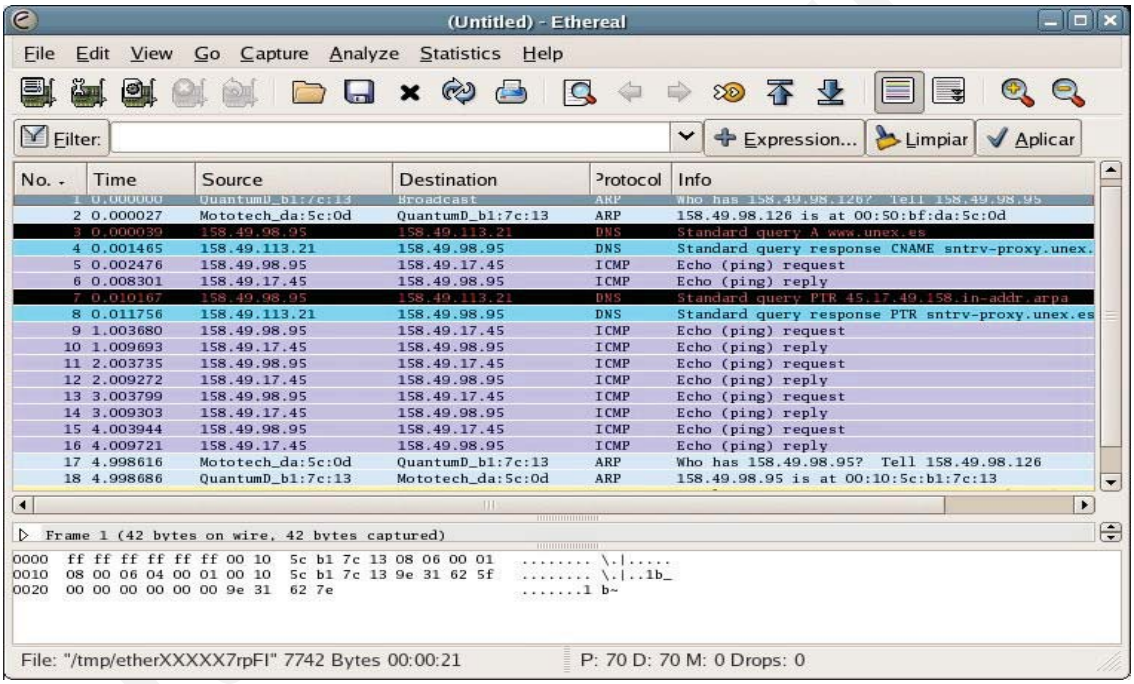
Worms:

- Slapper

9) Herramientas de seguridad en comunicaciones

- `Ethereal`: *http://www.ethereal.com/*
  - Análisis y visualización de la mayoría de protocolos en tiempo real.
  - Captura del tráfico de red en disco.
  - Aplicación de filtros de selección.
  - Visualización de contenido de datagramas, edición, modificación y selección interactiva en tiempo real.
  - Requerimientos:
    - Privilegios de root (*promiscuous mode*).
    - Librerías GTK+ para el entorno gráfico de la aplicación.
    - Librerías de interfaz LIBPCAP para acceso a placas de red.
    - Librerías del sistema GLIB.

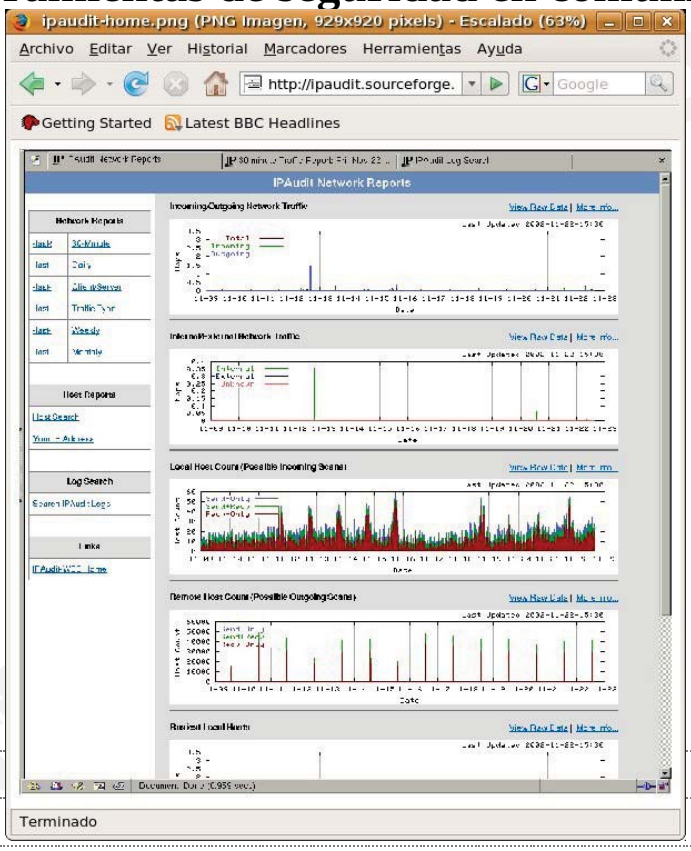
9) Herramientas de seguridad en comunicaciones



9) Herramientas de seguridad en comunicaciones

- `IPaudit WEB`: *http://ipaudit.sourceforge.net/ipaudit-web/*
  - Monitorización, generación y visualización de gráficas de tráfico.
  - Filtros y búsquedas potentes en los logs.
  - Almacen y busquedas en ficheros comprimidos (`gzip`).
  - Usa procesos cron cada 30 minutos.
  - Opcional el formato de datos para eliminar campos no deseado (campo de datos).
  - Requerimientos:
    - Privilegios de root (promiscous mode) en una cuenta `ipaudit` para la instalación del software.
    - Librerías GNUPLOT para la generación de gráficos.
    - Librerías de interfaz LIBPCAP para acceso a placas de red.
    - Compliador de PERL para ejecutar scripts.
    - Servidor WWW que permita al usuario `ipaudit` visualización de páginas y ejecución de scripts.
    - Sistema debe permitir ejecución `cron` a los usuarios.

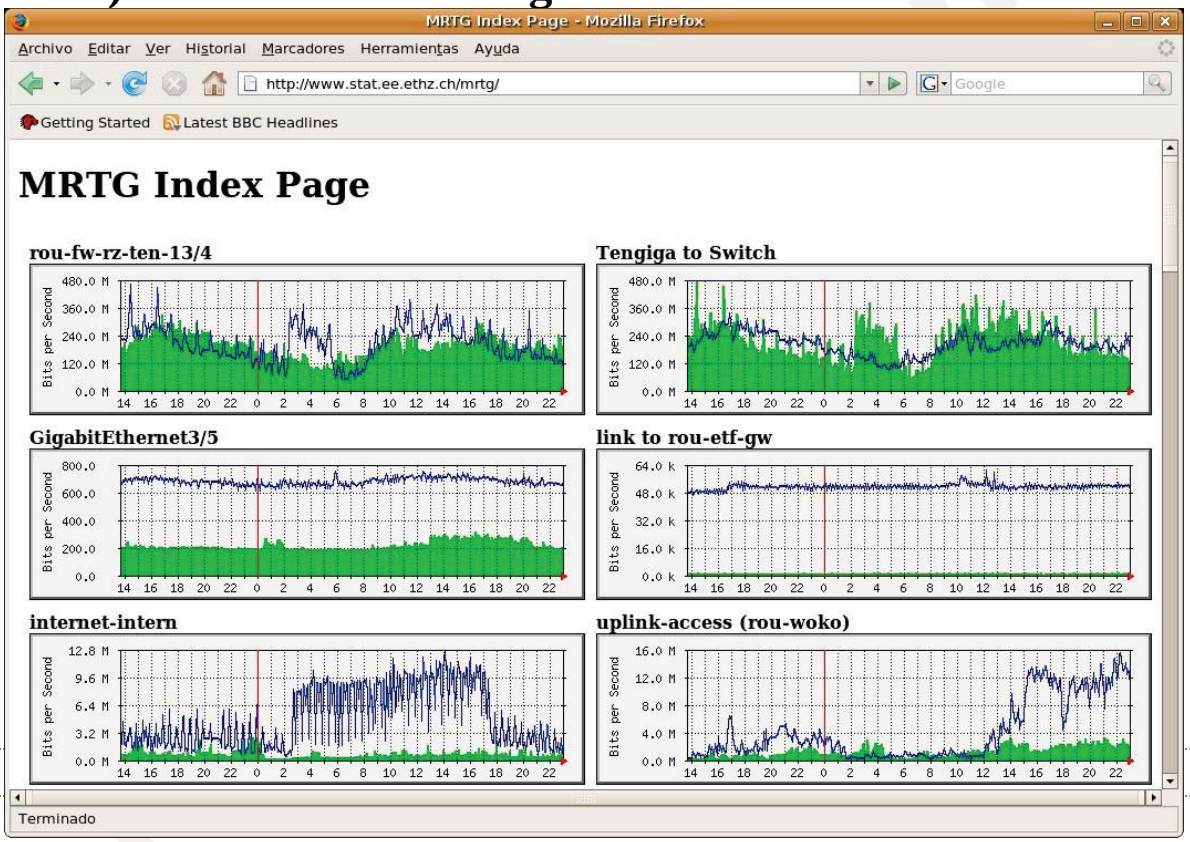
9) Herramientas de seguridad en comunicaciones



9) Herramientas de seguridad en comunicaciones

- `MRTG` (Multi Router Traffic Grapher) *http://oss.oetiker.ch/mrtg/*
  - Monitorización gráfica de las conexiones de red que reflejan el ancho de banda.
  - Se comunica con los dispositivos a través de SNMP.
  - Se usa normalmente para monitorizar dispositivos de red (routers y switches).
  - Complemento perfecto a IPaudit pues obtiene informes diarios, semanales, mensuales y anuales del ancho de banda.
  - Requerimientos:
    - Los dispositivos monitorizados deben tener activado el protocolo SNMP para que el software pueda conectarse y acceder a los datos.
    - Necesario un servidor de WWW.
    - Necesarias librerías LIBPNG para la creación de imagenes en formato PNG.
    - Sistema debe permitir ejecución `cron` a los usuarios pues requiere la ejecución de scripts cada cinco minutos.

9) Herramientas de seguridad en comunicaciones

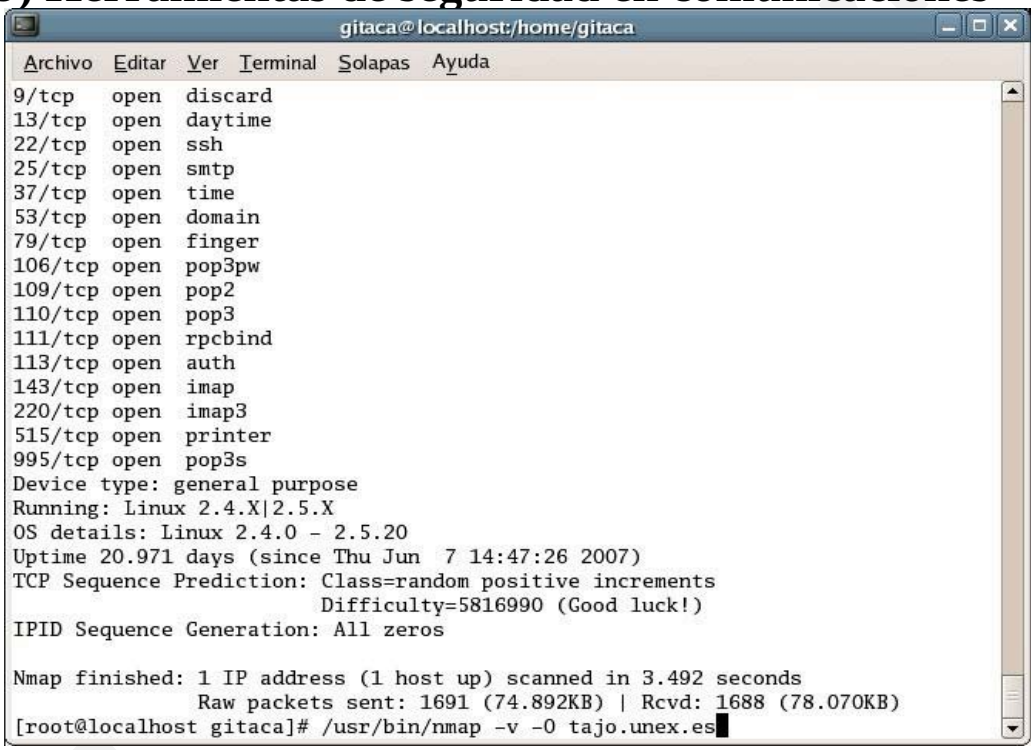


Administración Avanzada de Redes TCP/IP

9) Herramientas de seguridad en comunicaciones

- NMAP (Network Mapper) http://insecure.org/nmap/
  - Exploración y auditoría de redes de ordenadores.
  - Realiza *port scanning* para localizar los servicios activos en un ordenador.
  - Puede usarse para asegurar que todo el tráfico proveniente de internet es monitorizado.
  - También puede usarse para hacer *OS fingerprinting* y averiguar el SO que está instalado en un ordenador.
  - Requerimientos:
    - Privilegios de root para ejecutarlo la mayor parte de opciones.

9) Herramientas de seguridad en comunicaciones

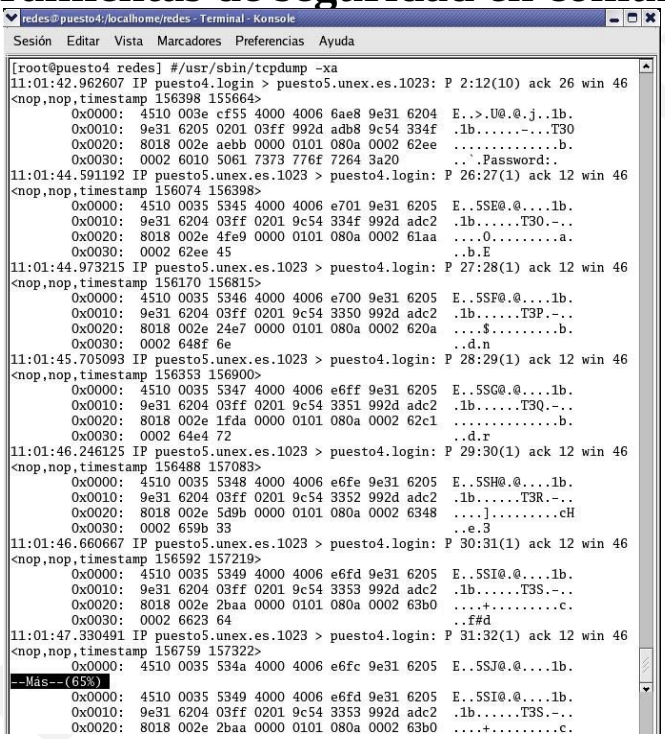


Administración Avanzada de Redes TCP/IP

9) Herramientas de seguridad en comunicaciones

- TCPdump *http://www.tcpdump.org*
  - Sniffer para la auditoría y adquisición de tráfico de red.
  - Permite el uso de filtros (protocolo, interfaz, @IP origen, @IP destino, port,...).
  - Diversas opciones de captura de cabeceras y datos.
  - IPaudit monitoriza por cabeceras, MRTG lo hace por tamaño de paquetes y tcpdump almacena junto a la cabecera el campo de datos, lo que permite reconstruir comunicaciones completas.
  - Los logs obtenidos pueden ser manipulados y visualizados por ethereal.
  - Requerimientos:
    - Privilegios de root para ejecutarlo.
    - Necesita la librería LIBPCAP para acceder a los dispositivos de red.
  - Puede complementarse con TCPreplay (*http://tcpreplay.sourceforge.net/*)

9) Herramientas de seguridad en comunicaciones



Administración Avanzada de Redes TCP/IP

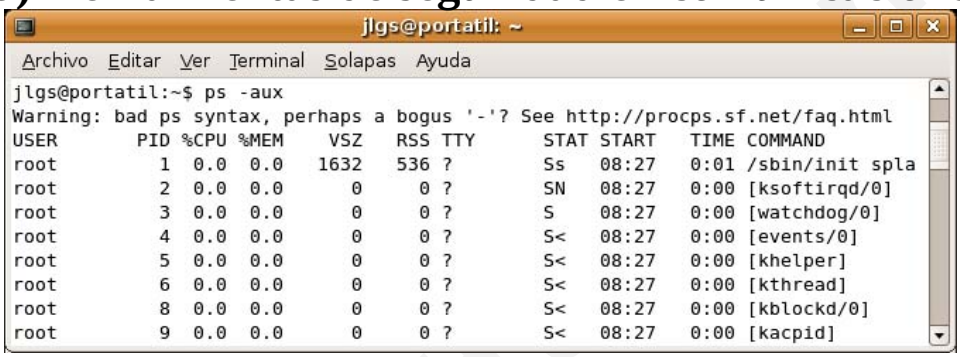
9) Herramientas de seguridad en comunicaciones

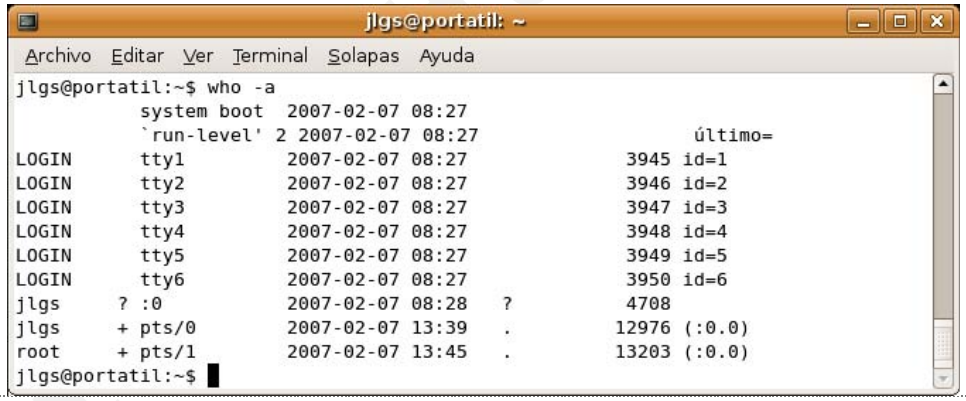
- Atentos a mensaje de *lastlogin*.
- Cuenta root sólo en consola de servidores: */etc/securetty*.
- Impedir comando *$su root* a usuarios concretos (en */etc/pam.d*).
- Si la seguridad es un requerimiento atención a NFS (evitar el acceso de escritura).
- Atención a *xinetd* para arrancar sólo los daemons necesarios.
- Configurar (firewall) tcp_wrappers con */etc/hosts.allow* y */etc/hosts.deny*
- Privilegios de */etc/init.d/* 700* para que sólo root tenga acceso.
- */etc/issue* y */etc/issue.net* aportan demasiada info.
- Editar archivo */etc/sysctl.conf*:
  - *net.ipv4.icmp_echo_ignore_all = 1*
  - *net.ipv4.tcp_syncookies = 1*
  - *net.ipv4.icmp_echo_ignore_broadcast = 1*

9) Herramientas de seguridad en comunicaciones

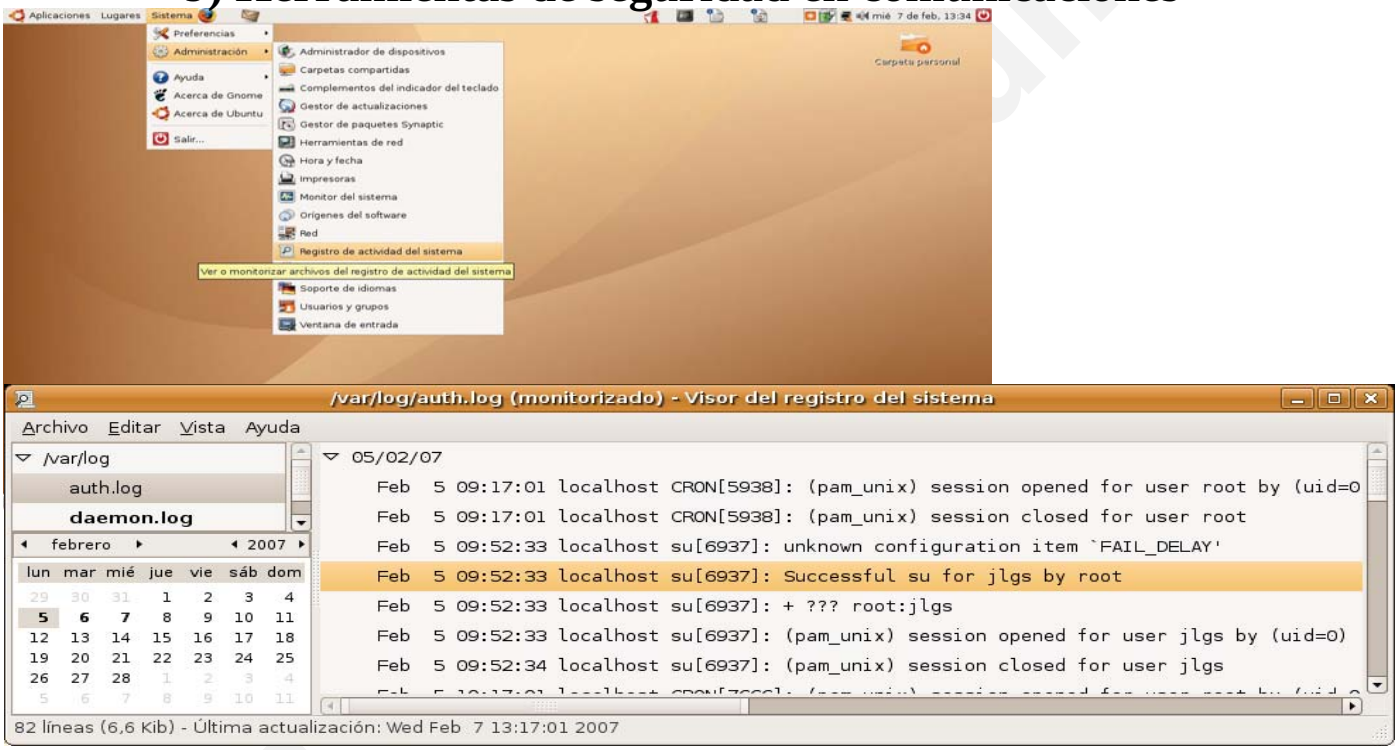
- *net.ipv4.conf.all.rp_filter = 1* . Activa protección contra IP spoofing
- *net.ipv4.conf.all.log_martians = 1*. Log de paquetes spoofed, redir.
- Encontrar archivos *.rhosts* en el sistema: *$find / -name .rhosts*
- Archivos en */etc/security* : permiten, limitan o controlan determinados accesos.

9) Herramientas de seguridad en comunicaciones





9) Herramientas de seguridad en comunicaciones



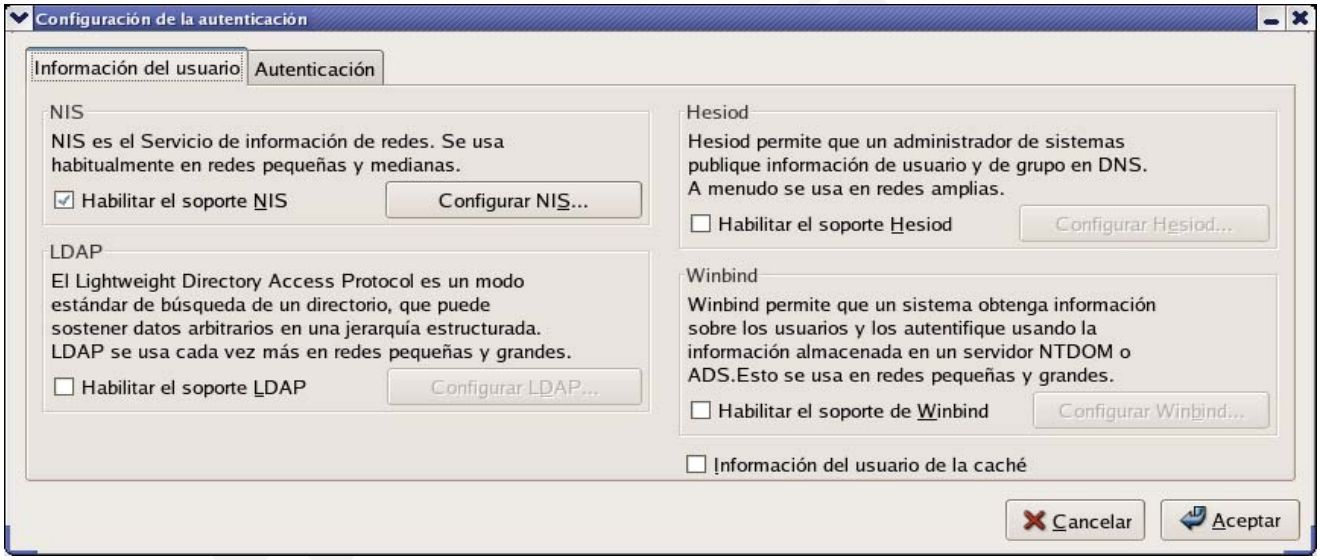
Nº 445

Administración Avanzada de Redes TCP/IP

9) Herramientas de seguridad en comunicaciones

Fedora Core 2.6.17-1.2142_FC4

system-config-authentication

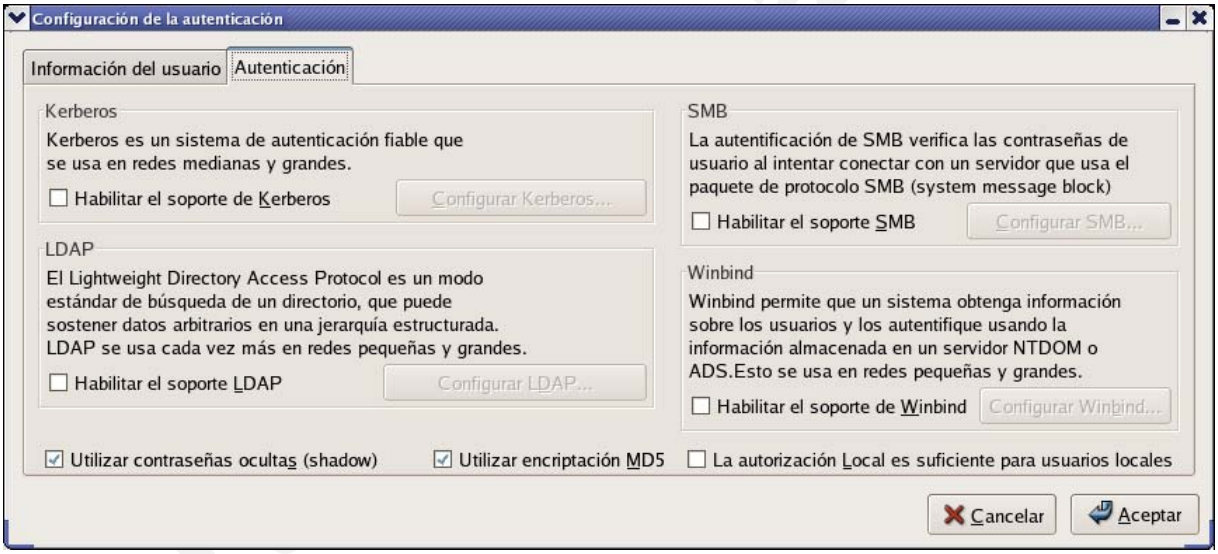


Nº 446

9) Herramientas de seguridad en comunicaciones

Fedora Core 2.6.17-1.2142_FC4

system-config-authentication



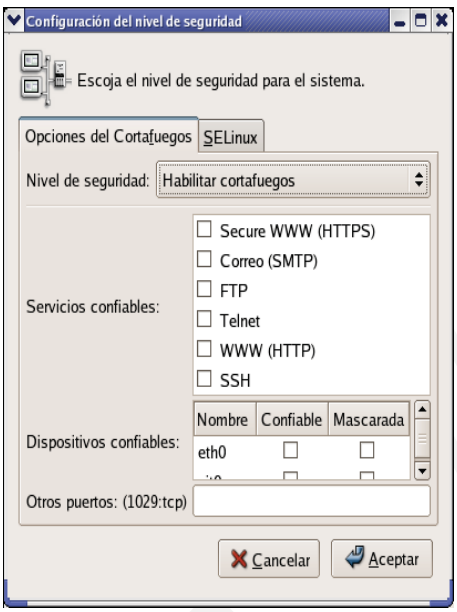
Nº 447

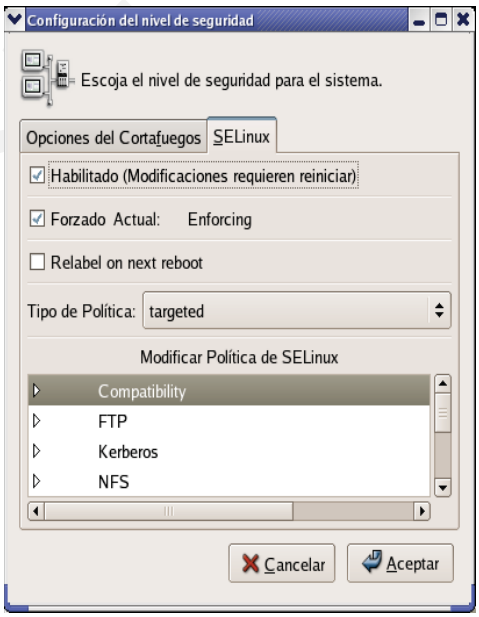
Administración Avanzada de Redes TCP/IP

9) Herramientas de seguridad en comunicaciones

Fedora Core 2.6.17-1.2142_FC4

system-config-securitylevel

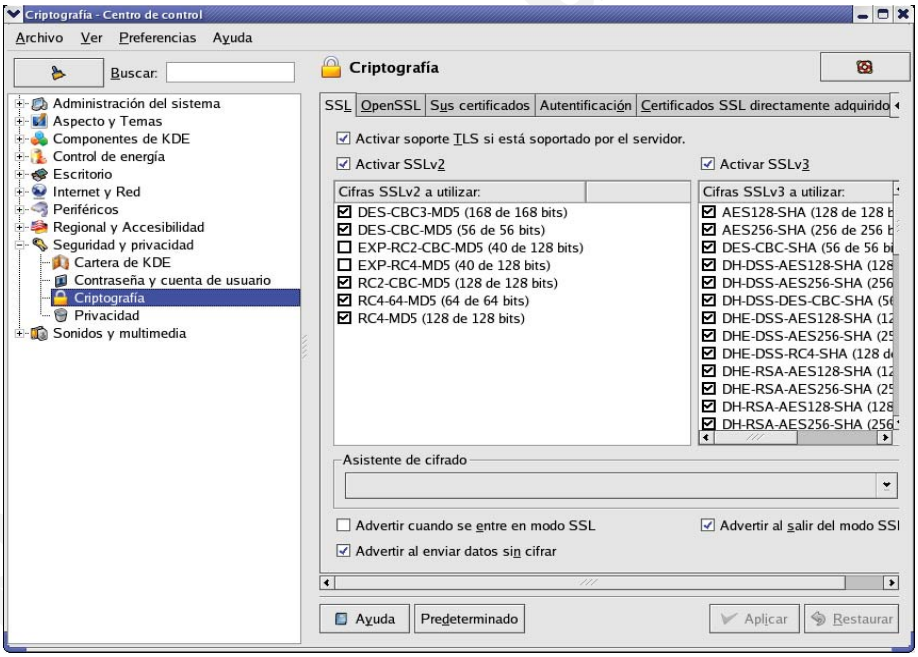




Nº 448

9) Herramientas de seguridad en comunicaciones

Fedora Core 2.6.17-1.2142_FC4



Administración Avanzada de Redes TCP/IP

9) Herramientas de seguridad en comunicaciones

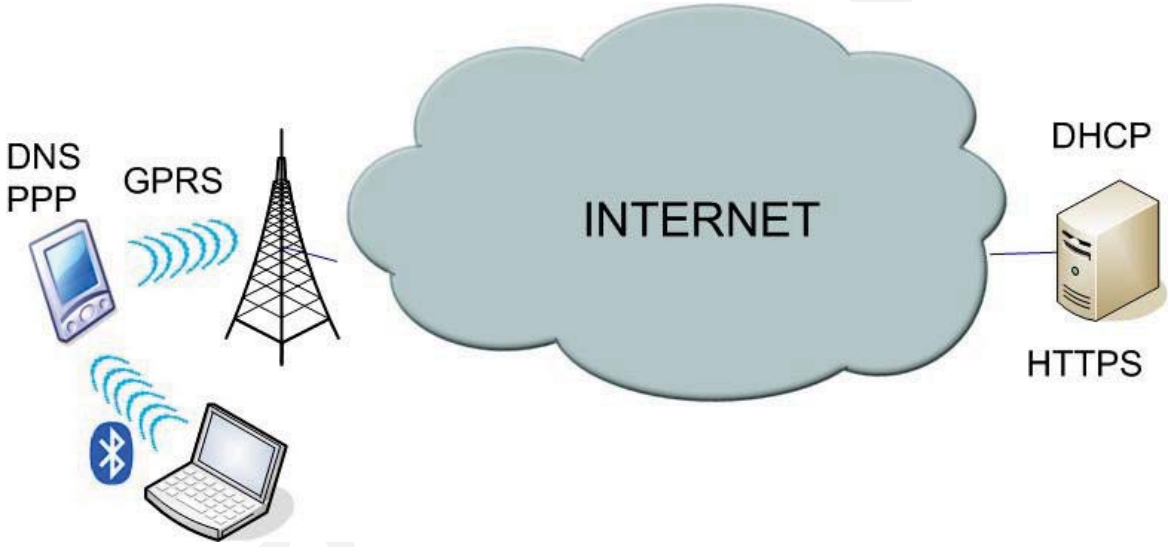
- *iptables* (evolución de *ipchains*):
  - *packet filtering*: tipo de firewall en el kernel de Linux.
  - un paquete llega a un sistema sólo si las reglas del cortafuegos lo permiten. Puede ser filtrado por: tipo, @origen, @destino o número de puerto.
  - usadas para configurar, mantener e inspeccionar las tablas de las reglas del filtrado de paquetes.
  - pueden definirse varias tablas y cada una puede tener varias cadenas que son una lista de reglas.
  - cada regla especifica qué hacer con un paquete que coincide con un patrón de filtrado.

10. Miscelánea de protocolos

Nº 451

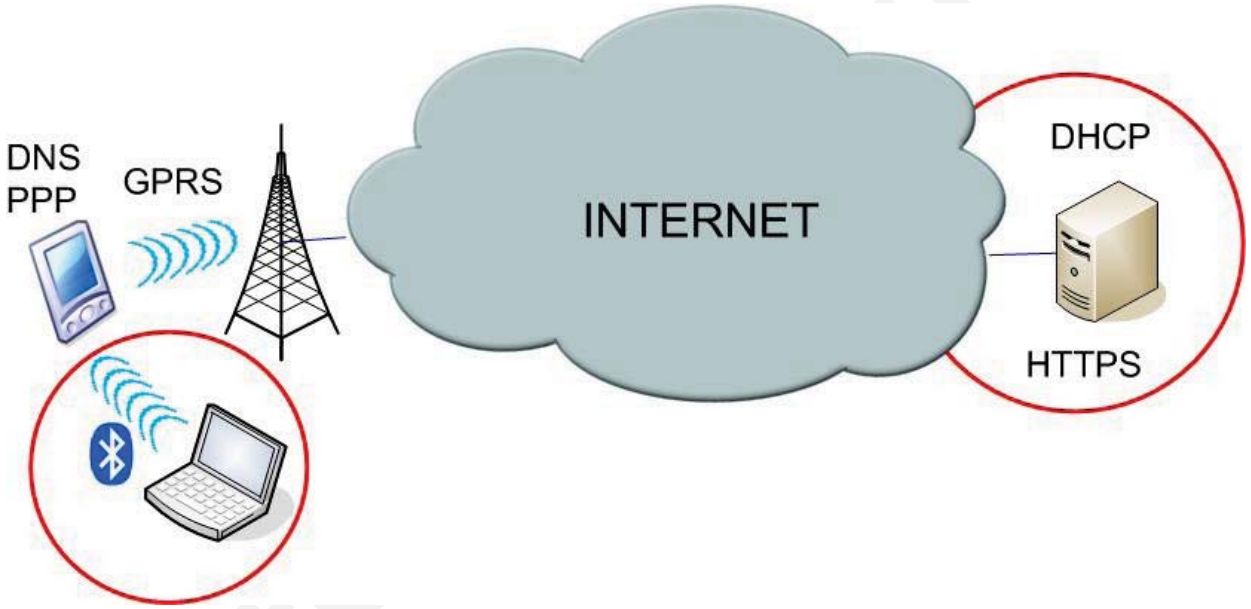
Administración Avanzada de Redes TCP/IP

Esquema de la conexión



Nº 452

Esquema de la conexión



Nº 453

Administración Avanzada de Redes TCP/IP

DHCP (I)

- DHCP (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 estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.
- Este protocolo se publicó en octubre de 1993, en el RFC 2131 . Los últimos trabajos van encaminados a IPv6 con el protocon el protocolo DHCPv6, en RFC 3315.
- El DHCP es sucesor de BOOTP (Bootstrap Protocol). Debido a que es un protocolo más avanzado, aunque BOOTP se sigue usando.
- DHCP recoge en su estándar tres módos de asignaciones de direcciones IP, asignación estática; asignación dinámica yasignación manual.

Nº 454

DHCP (II)

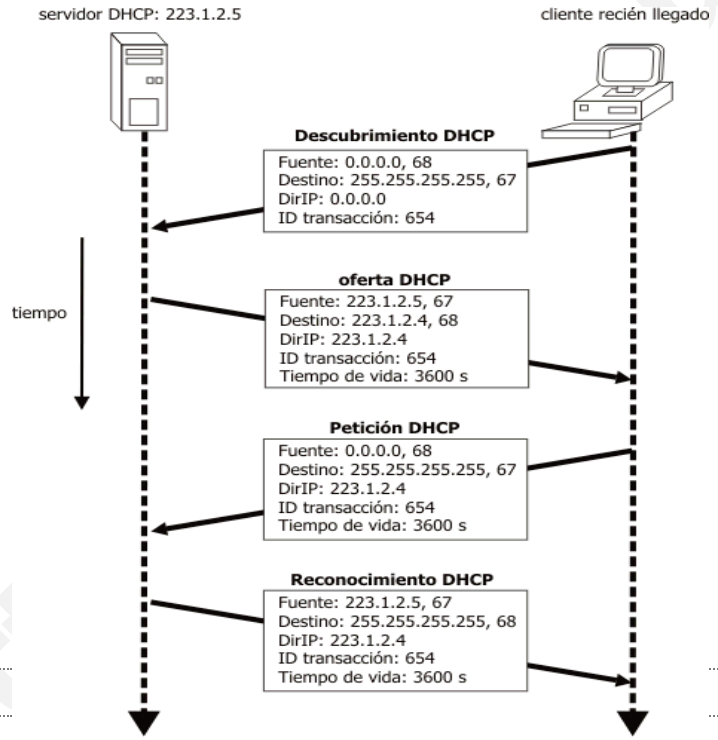
- DHCP usa los mismos puertos asignados por el IANA (Autoridad de Números Asignados en Internet según siglas en inglés) en BOOTP: 67/UDP para las computadoras servidor y 68/UDP para los clientes.
- DHCP Release: Los clientes envían una petición al servidor DHCP para liberar su dirección DHCP. Como los clientes generalmente no saben cuándo los usuarios pueden desconectarles de la red, el protocolo no define el envío del DHCP Release como obligatorio.
- DHCP Discover: Los clientes emiten peticiones masivamente en la subred local para encontrar un servidor disponible, mediante un paquete de broadcast. El router puede ser configurado para redireccionar los paquetes DHCP a un servidor DHCP en una subred diferente. La implementación cliente crea un paquete UDP con destino 255.255.255.255 y requiere también su última dirección IP conocida, aunque esto no es necesario y puede llegar a ser ignorado por el servidor.

Administración Avanzada de Redes TCP/IP

DHCP (III)

- DHCP Offer: El servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDRvbnv. El servidor especifica la dirección IP en el registro YIADDR. Como la cual se ha dado en los demás parámetros.
- DHCP Request: El cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor
- DHCP Acknowledge: Mensaje de confirmación y cierre desde el servidor hacia el cliente indicando los parámetros definitivos.
- DHCP Nack: El servidor envía al cliente un mensaje indicando que el contrato ha terminado o que la dirección IP asignada no es válida.
- DHCP Inform: El cliente envía una petición al servidor de DHCP: para solicitar más información que la que el servidor ha enviado con el DHCPACK original; o para repetir los datos para un uso particular.

DHCP (y IV)



BlueTooth (I)

- Es la la especificación IEEE 802.15.1 que define un estándar global de comunicación inalámbrica que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura, globalmente y sin licencia de corto rango. Los principales objetivos que se pretende conseguir con esta norma son:
  - Facilitar las comunicaciones entre equipos móviles y fijos.
  - Eliminar cables y conectores entre éstos.
  - Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.
- La especificación de Bluetooth define un canal de comunicación de máximo 720 kb/s (1 Mbps de capacidad bruta) con rango óptimo de 10 metros (opcionalmente 100 m con repetidores).
- La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex con lo que se tienen total de 79 frecuencias con intervalos de 1Mhz

BlueTooth (II)

- Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se puede implementar en un solo chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9 mm y que consume aproximadamente 97% menos energía que un teléfono móvil común.
- El protocolo de banda base (canales simples por línea) combina conmutación de circuitos y paquetes. Para asegurar que los paquetes no lleguen fuera de orden, los slots pueden ser reservados por paquetes síncronos, un salto diferente de señal es usado para cada paquete. Por otro lado, la conmutación de circuitos puede ser asíncrona o síncrona. Tres canales de datos síncronos (voz), o un canal de datos síncrono y uno asíncrono, pueden ser soportados en un solo canal. Cada canal de voz puede soportar una tasa de transferencia de 64 kb/s en cada sentido, la cual es suficientemente adecuada para la transmisión de voz. Un canal asíncrono puede transmitir como mucho 721 kb/s en una dirección y 56 kb/s en la dirección opuesta, sin embargo, para una conexión asíncrona es posible soportar 432,6 kb/s en ambas direcciones si el enlace es simétrico.

Nº 459

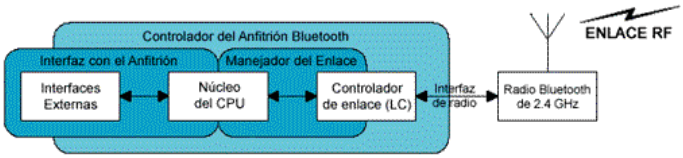
Administración Avanzada de Redes TCP/IP

BlueTooth (III)

- El Hardware que compone el dispositivo Bluetooth esta compuesto por dos partes:
  - un dispositivo de radio, encargado de modular y transmitir la señal
  - un controlador digital, compuesto por una CPU, por un procesador de señales digitales (DSP - Digital Signal Processor) llamado Link Controller (o controlador de Enlace) y de los interfaces con el dispositivo anfitrión.
- El LC o Link Controller es el encargado del procesamiento de la banda base y del manejo de los protocolos ARQ y FEC de capa física. Además, se encarga de las funciones de transferencia (tanto asíncrona como síncrona), codificación de Audio y cifrado de datos.
- La CPU del dispositivo se encarga de atender las instrucciones relacionadas con Bluetooth del dispositivo anfitrión, para así simplificar su operación. Para ello, sobre el CPU corre un software denominado Link Manager que tiene la función de comunicarse con otros dispositivos por medio del protocolo LMP.

Nº 460

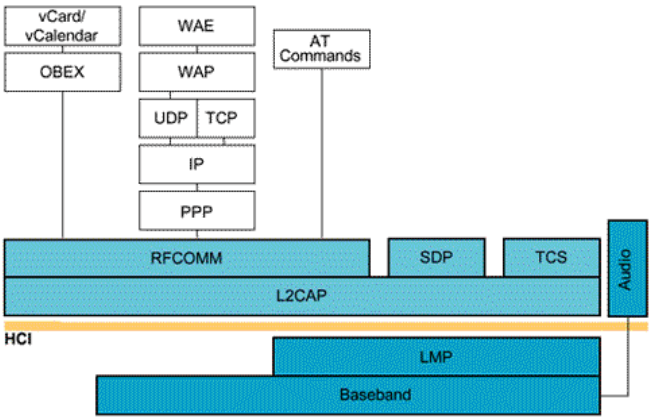
BlueTooth (IV)



- Entre las tareas realizadas por el LC y el Link Manager, destacan las siguientes:
  - Envío y Recepción de Datos.
  - Empaginamiento y Peticiones.
  - Determinación de Conexiones.
  - Autenticación.
  - Negociación y determinación de tipos de enlace, por ejemplo SCO o ACL
  - Determinación del tipo de cuerpo de cada paquete.
  - Ubicación del dispositivo en modo sniff o hold.

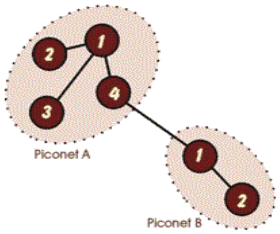
BlueTooth (V)

- Buscando ampliar la compatibilidad de los dispositivos Bluetooth, los dispositivos que se apegan al estándar utilizan como interfaz entre el dispositivo anfitrión (portatil, teléfono móvil, etc) y el dispositivo Bluetooth como tal (chip Bluetooth) con una interfaz denominada HCI (Host Controller Interface).



BlueTooth (VI)

- Los protocolos de alto nivel como el SDP (Protocolo utilizado para encontrar otros dispositivos Bluetooth dentro del rango de comunicación), RFCOMM (Protocolo utilizado para emular conexiones de puerto serie) y TCS (Protocolo de control de telefonía) interactúan con el controlador de banda base a través del Protocolo L2CAP (Logical Link Control and Adaptation Protocol). El protocolo L2CAP se encarga de la segmentación y reensamblaje de los paquetes para poder enviar paquetes de mayor tamaño a través de la conexión Bluetooth.
- Las redes creadas con dispositivos bluetooth pueden ser punto a punto o multipunto.



BlueTooth (VII)

- Los dispositivos, se comunican en redes denominadas piconets. Estas redes tienen posibilidad de crecer hasta tener 8 conexiones punto a punto. Además, se puede extender la red mediante la formación de scatternets. Una scatternet es la red producida cuando dos dispositivos pertenecientes a dos piconets diferentes, se conectan.
- En una piconet, un dispositivo debe actuar como master, enviando la información del reloj (para sincronizarse) y la información de los saltos de frecuencia. El resto de los dispositivos actúan como slaves.
- Bluetooth esta diseñado para usar acuses de recibos (acknowledgement) y saltos de frecuencias (frecuency hopping), lo cual hará conexiones robustas. Esto esta basado en paquetes, y saltarán a una nueva frecuencia después de que cada paquete es recibido, lo cual no solo ayuda a los problemas de interferencia, sino que añade seguridad. La tasa de datos es un megabytes/segundo, incluyendo el encabezado. Una transmisión "full duplex" (ambas direcciones al mismo tiempo) es realizado por multiplexaje de división de tiempo.

BlueTooth (VIII)

- Como se especificó previamente, la transmisión de datos puede ser realizada de maneta síncrona o asíncrona. El método Síncrono Orientado a Conexión (SCO) es usado principalmente para voz, y el Asíncrono No Orientado a Conexión (ACL) es principalmente usado para transmitir datos. Dentro de un "piconet" cada par master-slave pueden usar un modo de transmisión distinto, y los modos pueden ser cambiados en algún momento. La división de tiempo "Duplex", es usado para SCO y ACL, y ambos soportan 16 tipos de paquetes, cuatro de los cuales son paquetes de control, que son los mismos en cada tipo . Debido a la necesidad de tranquilidad en la transmisión de datos, los paquetes SCO son entregados en intervalos reservados, esto es, los paquetes son enviados en grupos sin permitir la interrupción de otras transmisiones. Los enlaces ACL soportan tanto transmisión simétrica como transmisión asimétrica.

BlueTooth (IX)

- Las conexiones Bluetooth, son establecidas a través de la siguiente técnica:
- Standby: Los dispositivos en un "piconet" que no están conectados, están en modo standby, ellos escuchan mensajes cada 1,28 segundos, sobre 32 saltos de frecuencias.
- Page/Inquiry: Si un dispositivo desea hacer una conexión con otro dispositivo, éste le envía un mensaje de tipo page, si la dirección es conocida; o una petición a través de un mensaje de page, si éste no es conocido. La unidad "master" envía 16 page message idénticos, en 16 saltos de frecuencias, a la unidad "slave". Si no hay respuesta, el "master" retransmite en los otros 16 saltos de frecuencia. El método de Petición (inquiry) requiere una respuesta extra por parte de la unidad "slave", desde la dirección MAC, que no es conocida por la unidad "master".
- Active: Ocurre la transmisión de datos.
- Hold: Cuando el "master" o el "slave" lo piden, puede ser establecido un modo en el cual no son transmitidos datos. El objetivo de esto es conservar el poder.

BlueTooth (X)

  - Sniff: El modo sniff, es aplicable solo para las unidades "slaves", es para conserva el poder. Durante este modo, el "slave", no toma un rol activo en la "piconet", pero escucha a un reducido nivel.
  - Park: El modo park es un nivel más reducido, que el modo hold. Durante este, el "slave" es sincronizado a la "piconet", por eso no requiere un reactivación completa, pero no es parte del tráfico. En este estado, ellos no tienen direcciones MAC y solo escuchan para mantener su sincronización con el "master" y chequear los mensajes de broadcast.
- Tres técnicas de corrección de error han sido definidas:
  - 1/3 rate forward error correction code (FEC), este método es diseñado para reducir el número de retransmisión.
  - 2/3 rate forward error correction code FEC.
  - Automatic Repeat Request (ARQ).

Nº 467

Administración Avanzada de Redes TCP/IP

BlueTooth (XI)

- En cuanto a la Seguridad, ésta es provista en tres caminos:
  - A través de saltos de frecuencia pseudo-aleatorios que dificultan que dispositivos ajenos a la red puedan interceptar o ver el tráfico de información.
  - Autentificación, permite a un usuario controlar la conectividad para solo dispositivos especificados.
  - Encriptación, se usan claves secretas con longitudes de 1, 40 o 64 bits.
- Los modos de uso de bluetooth: Algunas de las aplicaciones que se pueden dar a los dispositivos Bluetooth han sido mencionadas en la especificación del estándar (versión 1). Entre otras, destacan las siguientes:
  - El Teléfono 3-en-1: Se ofrece la posibilidad de utilizar un mismo teléfono sin importar donde se encuentra. Puede funcionar como el teléfono en su casa, si el dispositivo está en el rango de las bases Bluetooth ubicadas en su casa, como teléfono móvil-portátil si no se encuentra cerca de las bases de su casa, y como medio de acceso a sus contactos, números de teléfono, email, etc.

Nº 468

BlueTooth (y XII)

- Conexión a Internet: El dispositivo Bluetooth puede conectarse con cualquier medio que esté conectado a Internet y que a la vez, posea una interfaz Bluetooth, para así mantenerlo siempre conectado, ya sea a través de su móvil, de su conexión dial-up o a través de una red cableada a Internet.
- Dispositivo Manos libres: El uso de este dispositivo permite acceder la información de los contactos, enviar correo electrónico y realizar llamadas sin ocupar las manos. Esta funcionalidad está controlada por voz.
- Portátil como teléfono: Se tiene la posibilidad de utilizar el portátil para realizar llamadas de voz tal cuál se haría con un teléfono..
- Sincronización automática: Constantemente, todos sus dispositivos Bluetooth mantienen sincronizada la información, de manera que si modifica alguna información en su portátil, y la misma estaba también almacenada en su PDA o en su móvil, el cambio se refleje allí también.
- Escritorio Inalámbrico: Bluetooth ofrece la posibilidad de eliminar todos los cables (excepto los de poder) que suelen invadir los escritorios, tanto en los hogares como en las oficinas.

Nº 469

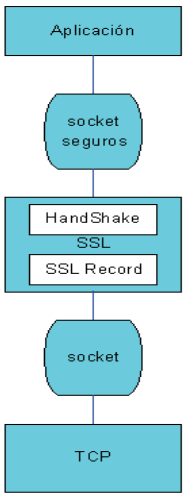
Administración Avanzada de Redes TCP/IP

HTTPS (I)

- El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es en este momento, cuando el navegador advierte que se están cargando elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS).
- SSL (SECURE SOCKET LAYER): Este protocolo fue creado por Netscape Communications para ofrecer seguridad y privacidad en Internet. Este protocolo soporta autenticación tanto de cliente como de servidor y además es independiente de la aplicación.
- En SSL existen dos partes:
- SSL Handshake: se encarga de realizar las funciones de autenticación entre cliente y servidor
- SSL Record: realiza el envío y recepción de datos, cifrado y descifrado.

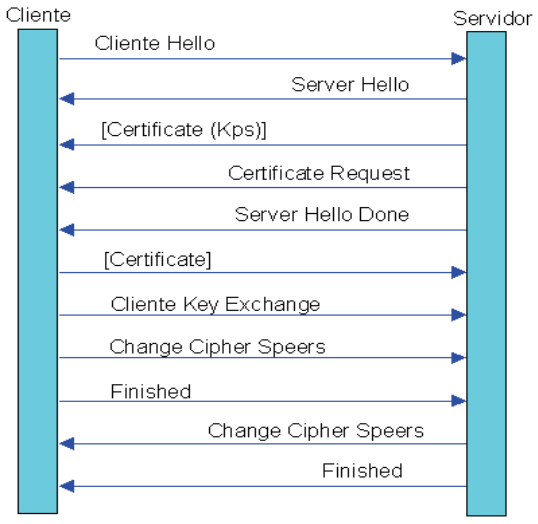
Nº 470

HTTPS (II)



HTTPS (III)

- En SSL la autenticación consiste en dos fases: la autenticación de servidor y la autenticación de cliente. La autenticación de cliente es opcional.



HTTPS (IV)

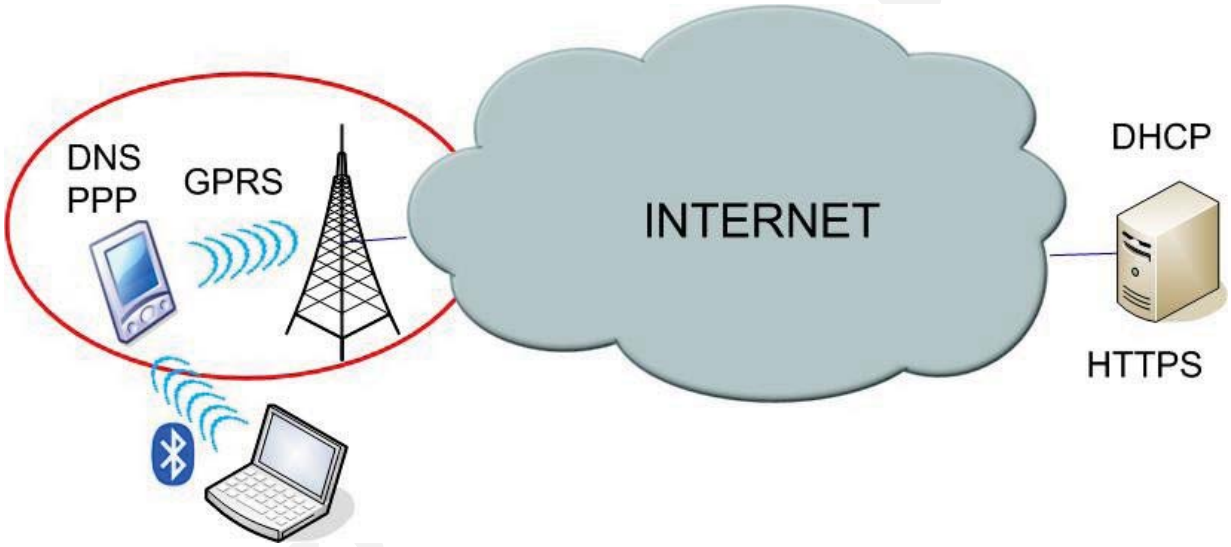
- El cliente envía al servidor los parámetros que quiere negociar y un número aleatorio creado por él (Cliente Hello). El servidor responde a los parámetros solicitados por el cliente y genera un número aleatorio que se le envía al cliente (Server Hello). A continuación el servidor envía su certificado al cliente y finaliza así la fase de autenticación (Server Hello Done). Opcionalmente, el servidor también puede pedir la autenticación del cliente, para ello el servidor pide el certificado al cliente (Certificate Request) y este se lo enviará (Certificate).
- Ahora el cliente genera una clave secreta que cifra con la clave pública del servidor. Esta clave cifrada se envía entonces al servidor (Cliente Key Exchange). El servidor descifra la clave secreta.
- En este punto, tanto el cliente como el servidor disponen de una clave secreta (clave de sesión simétrica) y por tanto se puede proceder al proceso de autenticación de forma segura (Change Cipher Speers y Finished). Esta clave es generada en cada sesión y cuando finaliza, se desecha.

Administración Avanzada de Redes TCP/IP

HTTPS (y V)

- Una característica importante de SSL es que una vez distribuida la clave de sesión se pueden establecer nuevas sesiones (cada una con una identificación distinta) sin necesidad de intercambiar dicha clave. Lo único que se hace es intercambiar información entre cliente y servidor cifrándola con la clave de sesión anteriormente distribuida y común para todas las sesiones.
- Características de SSL
- La SSL soporta una variedad de algoritmos criptográficos, incluidos los siguientes:
- La encriptación de clave pública RSA se utiliza durante la parte inicial del proceso
- RC2, RC4, IDEA, DES y triple DES pueden utilizarse después del intercambio inicial de claves para cifrar los datos a intercambiar.
- El algoritmo MD5 también se utiliza como parte del proceso de encriptación SSL.
- Por último y como nota practica, sabremos que estamos conectados a un sitio asegurado con SSL cuando en la URL aparezca https:// en vez de http://

Esquema de la conexión

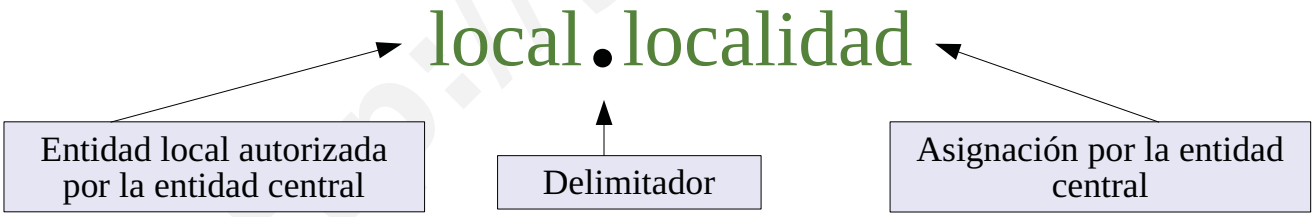


DNS

- Los nodos en Internet son identificados por su dirección IP.
- Este mecanismo es “engorroso” para un usuario.
  - Se utilizan nombres alfanuméricos
- Inicialmente, existía un sistema que mantenía la relación de nombres a direcciones en un fichero (/etc/hosts), que se obtenía a través de FTP.
  - Se llamaba espacio de nombres plano.
  - Con el crecimiento de la red, aparecieron problemas de escalabilidad
- La siguiente solución es el uso de servidores DNS (*Domain Name System*), que resuelven y traducen los nombres a direcciones IP.
- DNS es un sistema de bases de datos distribuida.
- Jerárquico, basado en un esquema de nombres de dominio.
  - Sistema escalable.

DNS. Nombres Jerárquicos.

- El sistema de nombres jerárquicos permite un crecimiento rápido y extenso del conjunto de nombres, sin una entidad central administradora
- Características
  - Permite la transformación eficiente
  - Facilita la delegación de autoridad
- Garantiza un control autónomo de la asignación de los nombres
- El nombre es particionado:



DNS. Nombres Jerárquicos.

- La autoridad correspondiente puede subdividir el espacio de nombres en cada nivel.
  - La idea es conservar subdividido el espacio de nombres hasta que este sea manejable
- Nombres de dominio oficiales:

Nombre del Dominio	Significado
COM	Organizaciones comerciales
EDU	Instituciones educativas
GOV	Instituciones gubernamentales
MIL	Grupos militares
NET	Centros de soporte de red
ORG	Organizaciones
ARPA	Dominio de ARPANET (obsoleto)
INT	Organizaciones Internacionales
TV	Televisiones - Nuevo

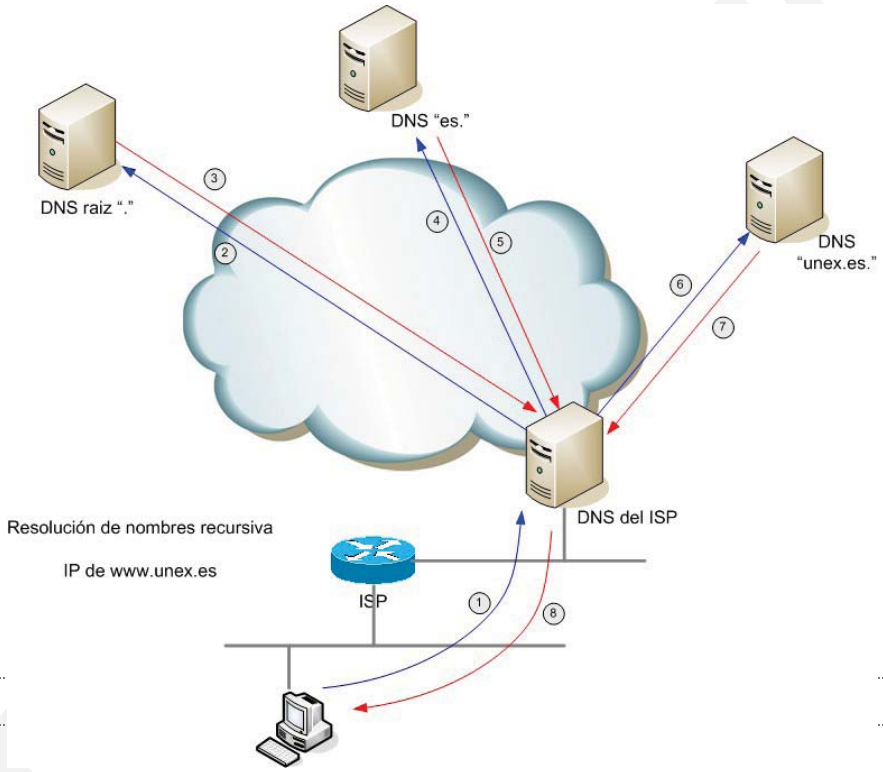
DNS. Funcionamiento.

- Dos posibilidades en la resolución de nombres.
- Recursiva
  - Se pregunta a un servidor.
  - Si la sabe, devuelve la respuesta.
  - Si no la sabe, pregunta a otro servidor y cuando recibe la respuesta la reenvía al usuario.
- Iterativa
  - Se pregunta a un servidor.
  - Si la sabe, retorna la respuesta
  - Si no la sabe, devuelve la dirección del servidor al que hay que preguntar
  - Hay que preguntar nuevamente.

Nº 479

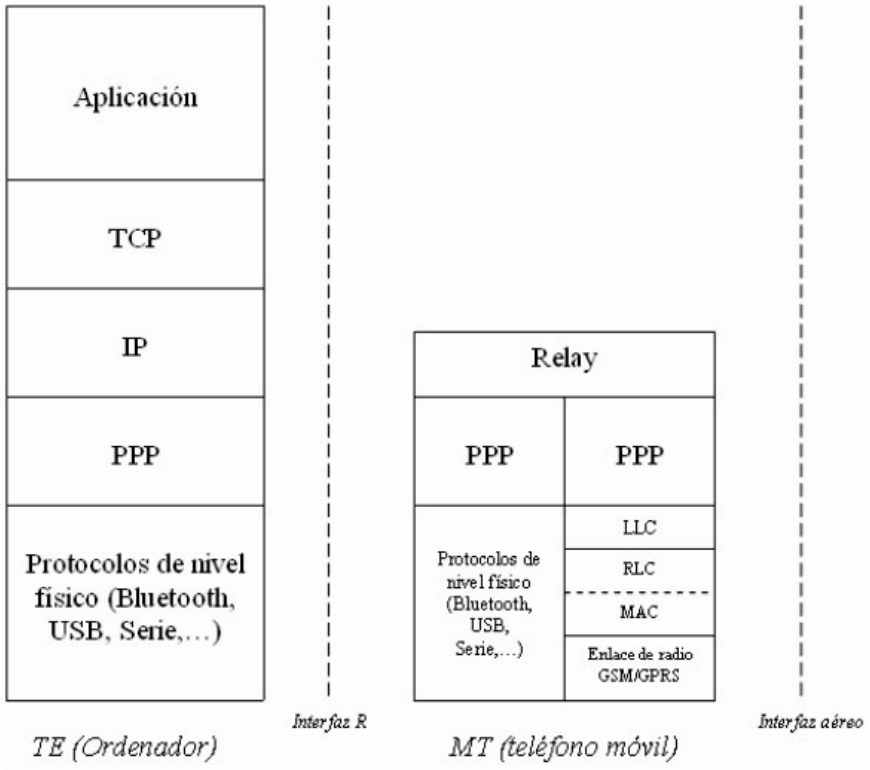
Administración Avanzada de Redes TCP/IP

DNS. Funcionamiento.



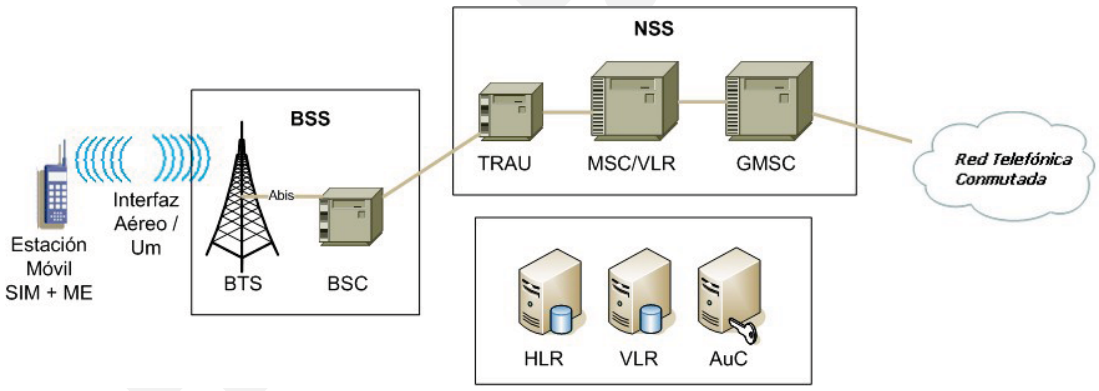
Nº 480

Tecnologías de acceso en comunicaciones móviles



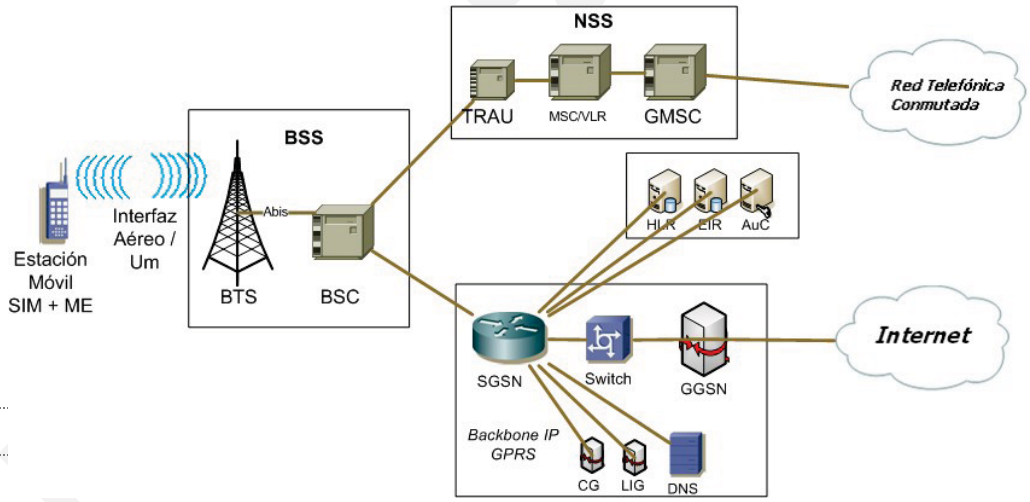
Tecnologías de acceso en comunicaciones móviles

- GSM (2G)
  - Abarca el 82% del mercado global de las comunicaciones móviles tras el primer cuatrimestre de 2006. (Datos de *www.wirelessintelligence.com*).
  - Se producen 1000 conexiones nuevas por minuto.



Tecnologías de acceso en comunicaciones móviles

- GPRS (2.5G)
  - Responde a la demanda de nuevos servicios *"non voice"*.
  - Núcleo de red de conmutación de paquetes más adecuado para el tráfico de datos.
  - Recursos compartidos entre los datos y la voz.

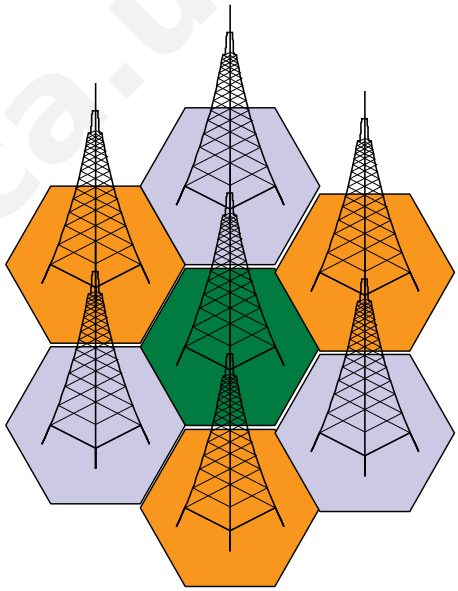


Tecnologías de acceso en comunicaciones móviles

- Redes de comunicaciones móviles de segunda generación utilizan una combinación de tecnoógias de acceso:
  - SDMA (*Space Division Multiple Access*)
  - TDMA (*Time Division Multiple Access*)
  - FDMA (*Frecuency Division Multiple Access*)

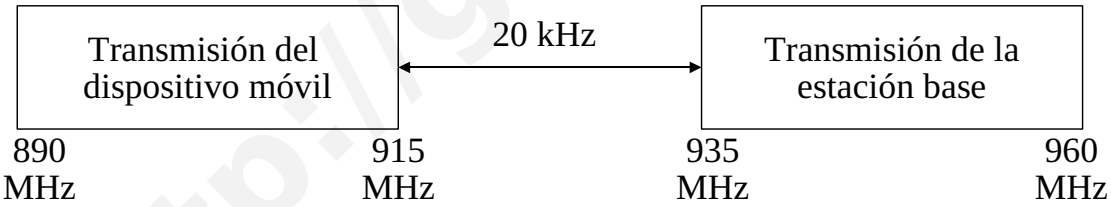
SDMA

- Proporciona la estructura de una red inalámbrica.
- Ventajas
  - Reusabilidad de frecuencias
  - Baja potencia de transmisión necesitadas por los móviles.
- Desventajas
  - Estructura más compleja que con una sola estación.



FDMA

- FDMA es una técnica de acceso múltiple.
- Cada banda de frecuencia es dividida en canales individuales.
- GSM trabaja en las bandas de 900, 1800 y 1900 MHz.
- En GSM, un canal necesita 2 x 200 kHz.
- 25 MHz / 200 kHZ = 125 canales disponibles

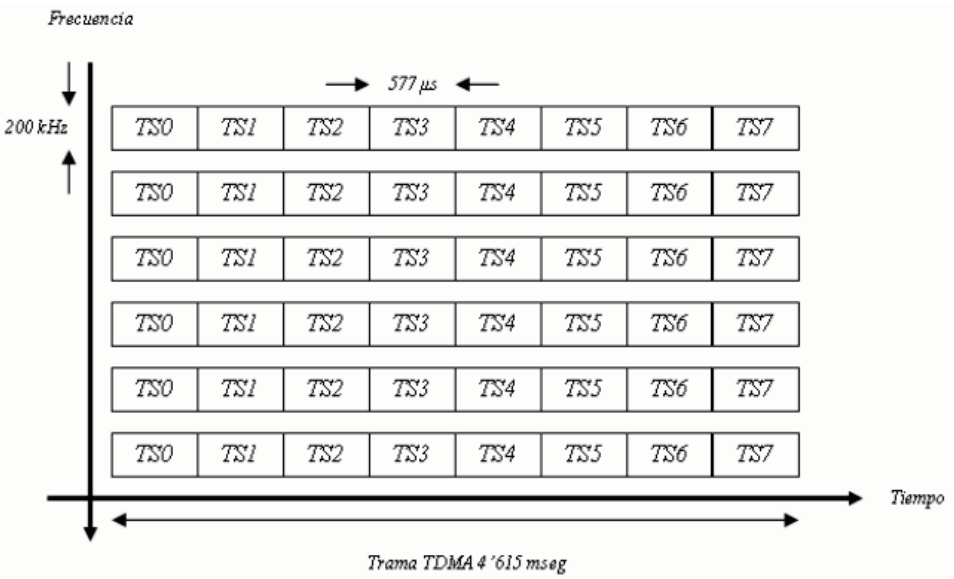


TDMA

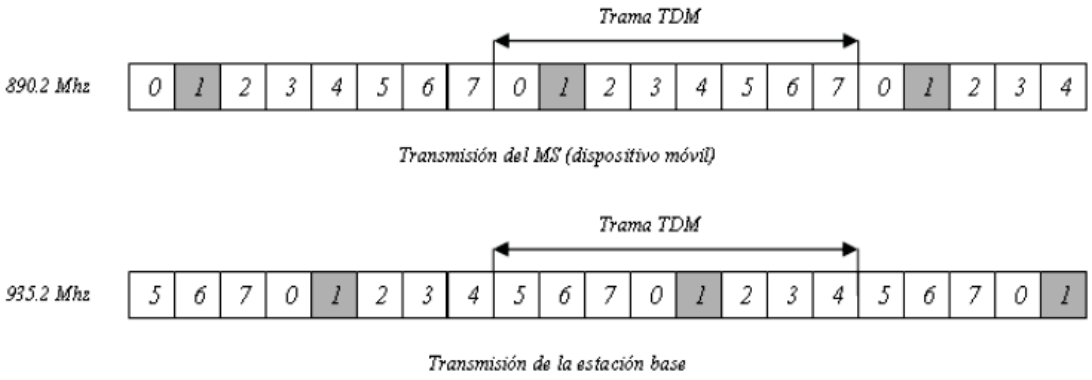
- Con FDMA, en una conexión activa, un cliente recibe un canal de frecuencia exclusivo para su uso durante la llamada.
- Con TDMA, cada canal de frecuencia es dividido y cada cliente tiene derecho de acceso a un canal durante una conexión por un corto, pero repetido espacio de tiempo.
- Cada intervalo que se repite se llama *time-slot*.
- Da la impresión de una conexión ininterrumpida.
- En GSM / GPRS, cada canal de frecuencia se divide en ocho *time-slots*
- Se comparte el tráfico de datos con el de voz.

Administración Avanzada de Redes TCP/IP

TDMA



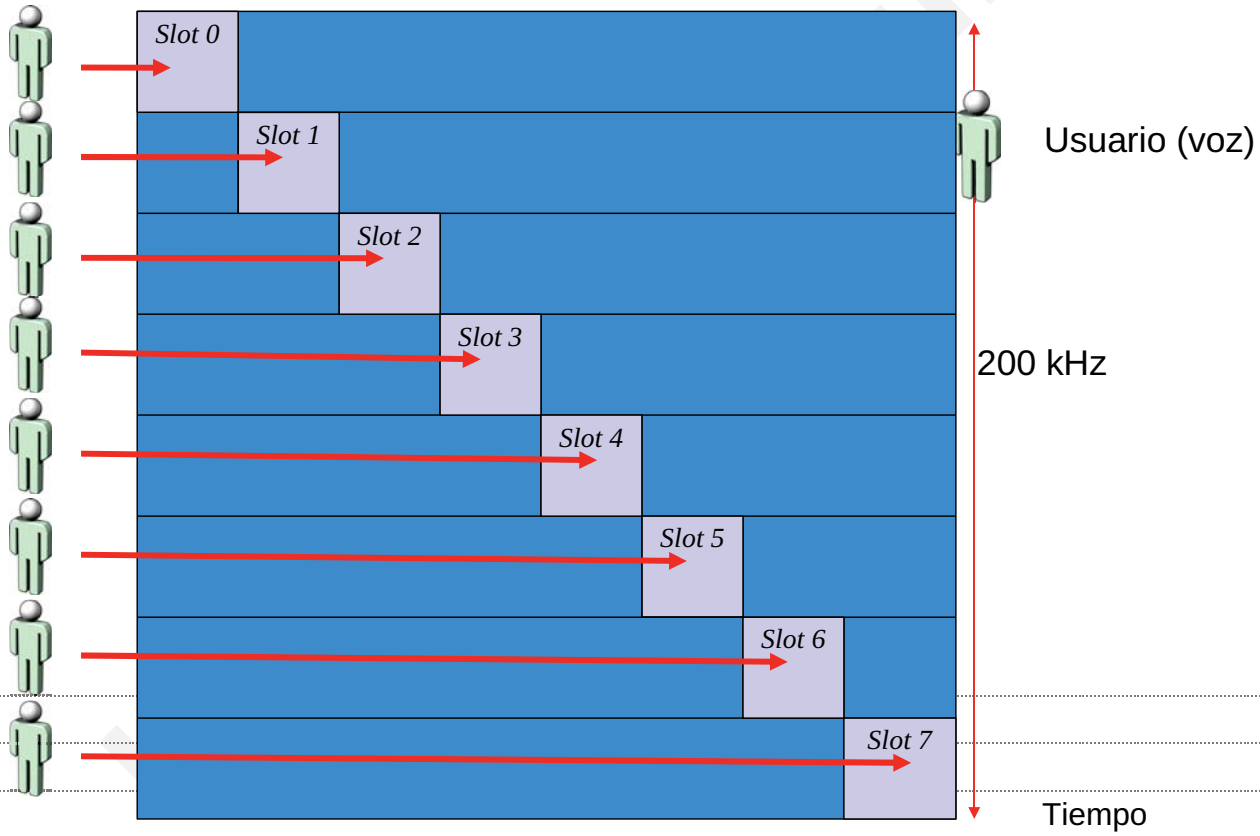
TDMA



Nº 489

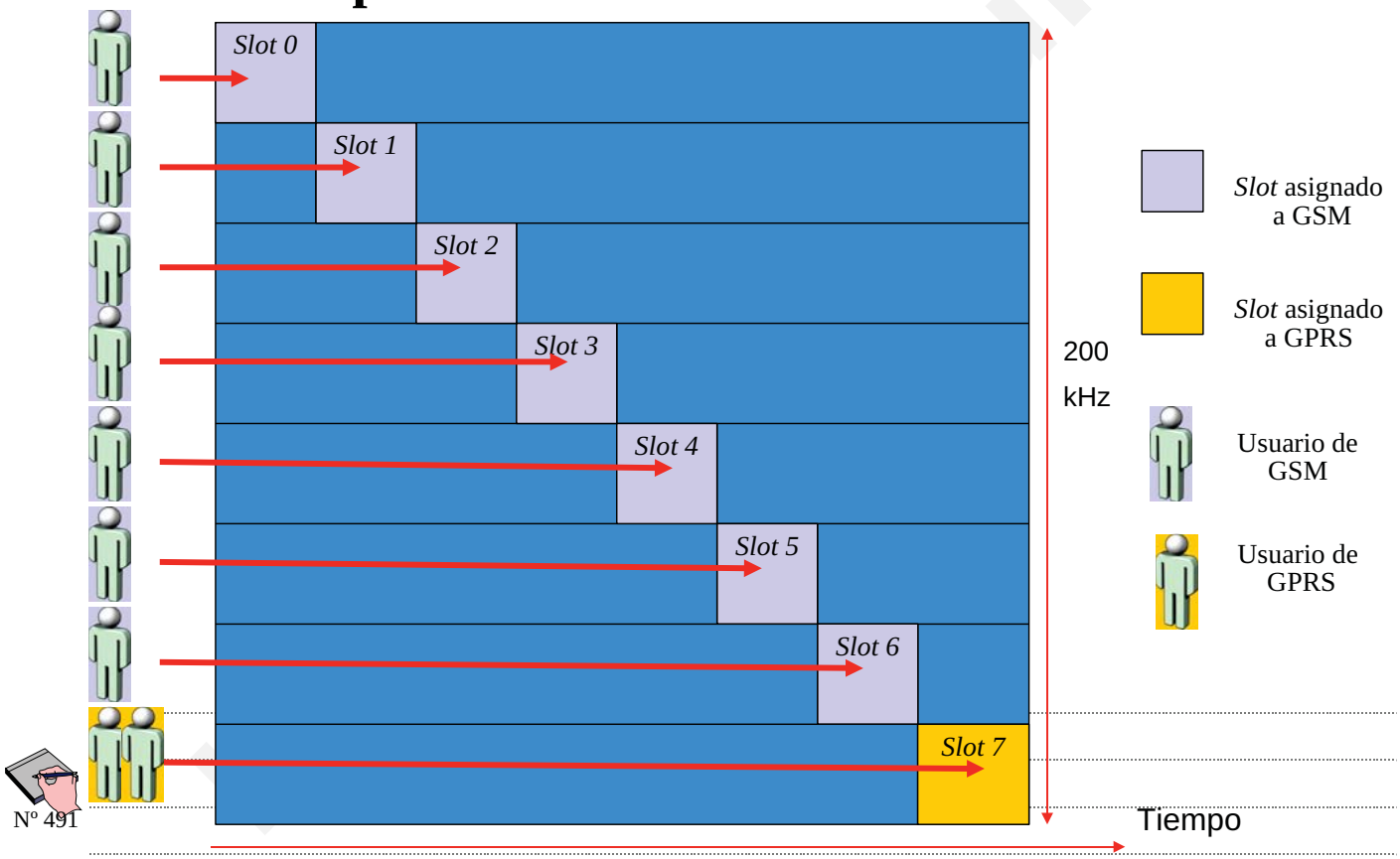
Administración Avanzada de Redes TCP/IP

Compartición de recursos GSM / GPRS



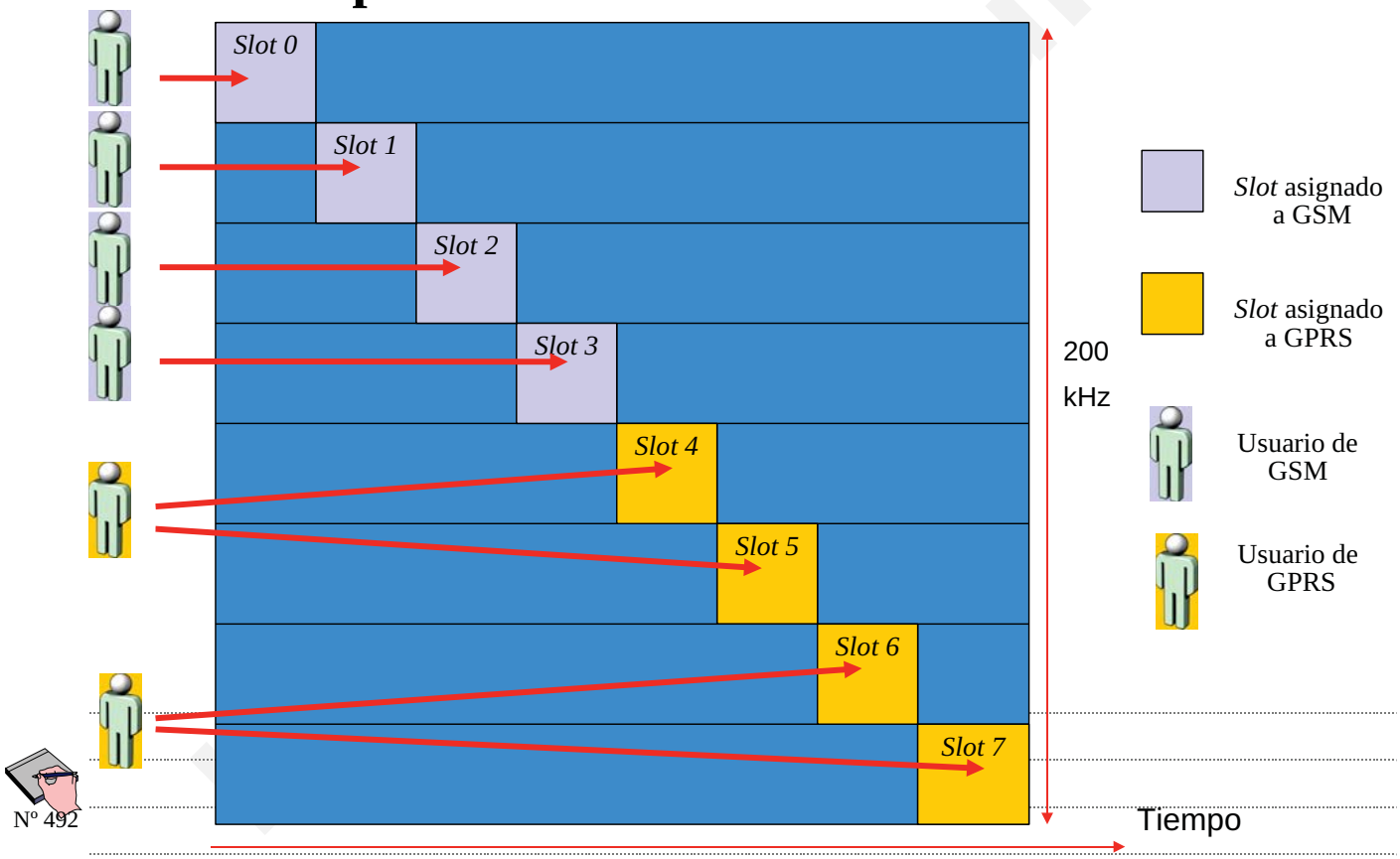
Nº 490

Compartición de recursos GSM / GPRS



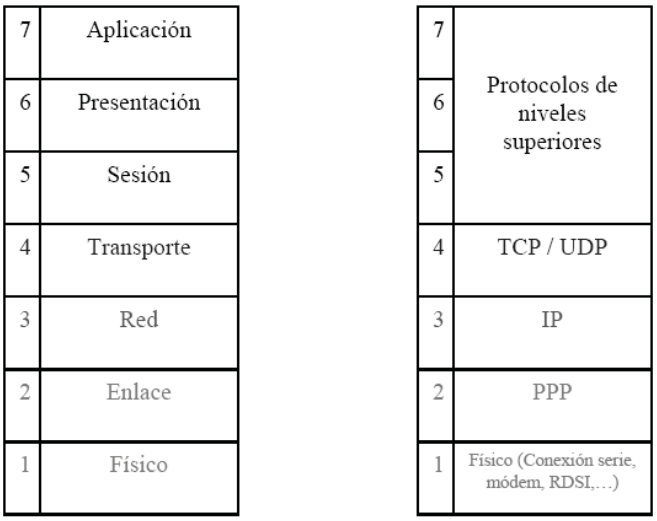
Administración Avanzada de Redes TCP/IP

Compartición de recursos GSM / GPRS



PPP

- PPP es un protocolo orientado a conexión, que permite enlaces sobre el nivel 2 de distintas conexiones de nivel físico.
- Fue diseñado para transportar tráfico IP. pero es común permitir que cualquier tipo de datagrama de la capa de red sea enviado sobre una conexión PPP.
- PPP se ajusta a la capa de enlace (y física) en el modelo TCP/IP, como muestra la imagen siguiente.



PPP. Componentes y funcionamiento

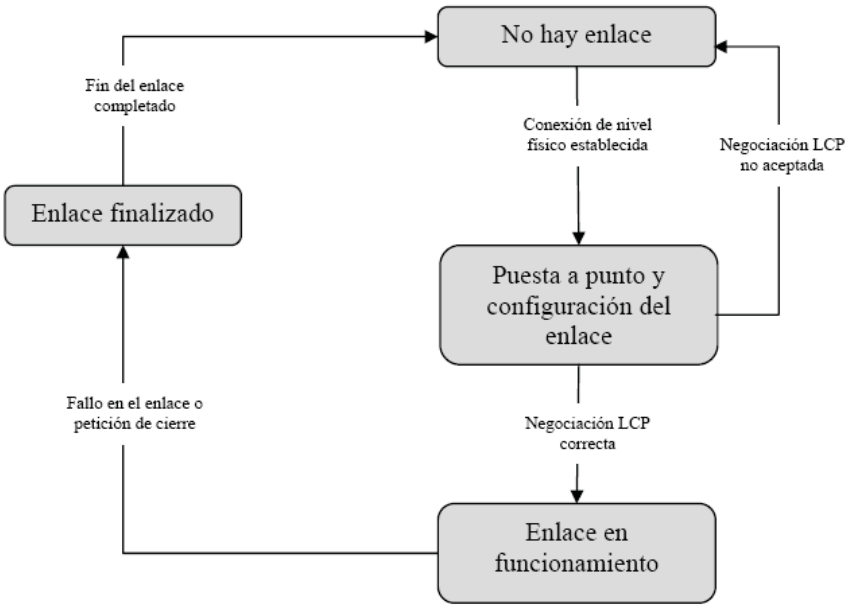
- Podemos distinguir 3 componentes:
  - Método de Encapsulación PPP: El trabajo principal de PPP es coger mensajes de las capas superiores como datagramas IP y encapsularlos para transmitirlos sobre la capa física
  - *Link Control Protocol* (LCP): El protocolo LCP es responsable de establecer, mantener y finalizar el enlace entre los dispositivos.
  - *Network Control Protocols* (NCPs):
    - PPP soporta la encapsulación de muchos tipos de datagramas del nivel tres.
    - Después de la configuración del enlace a cargo de LCP, el control es pasado al NCP específico para el protocolo de nivel tres que vaya a ser transferido en el en lace PPP.
    - Por ejemplo, cuando se transfiere IP sobre PPP, el NCP utilizado es el Internet Protocol Control Protocol (IPCP).

PPP. Componentes y funcionamiento

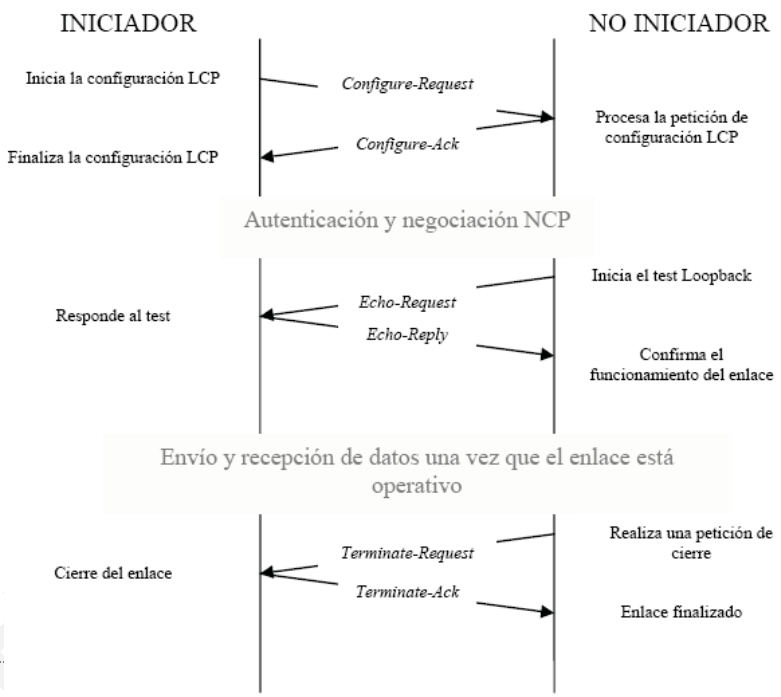
- Funcionamiento general implica tres pasos básicos.
  - Configuración y puesta a punto del enlace:
    - Antes de intercambiar información, hay que levantar un enlace.
    - LCP comienza este proceso, ayudado de otros como la autenticación.
    - Una vez el enlace activado, se pasa el control al NCP adecuado.
  - Funcionamiento del enlace:
    - Cada dispositivo realiza el envío cogiendo los datagramas, los encapsula y los envía por la capa física.
    - Al recibir información, las tramas PPP se toman de la capa física, se quita la cabecera PPP y se pasa el datagrama al nivel 3.
  - Finalización del enlace: Cuando cualquiera de los dos dispositivos decidan finalizar la comunicación, el enlace finalizará..

Administración Avanzada de Redes TCP/IP

PPP. Componentes y funcionamiento



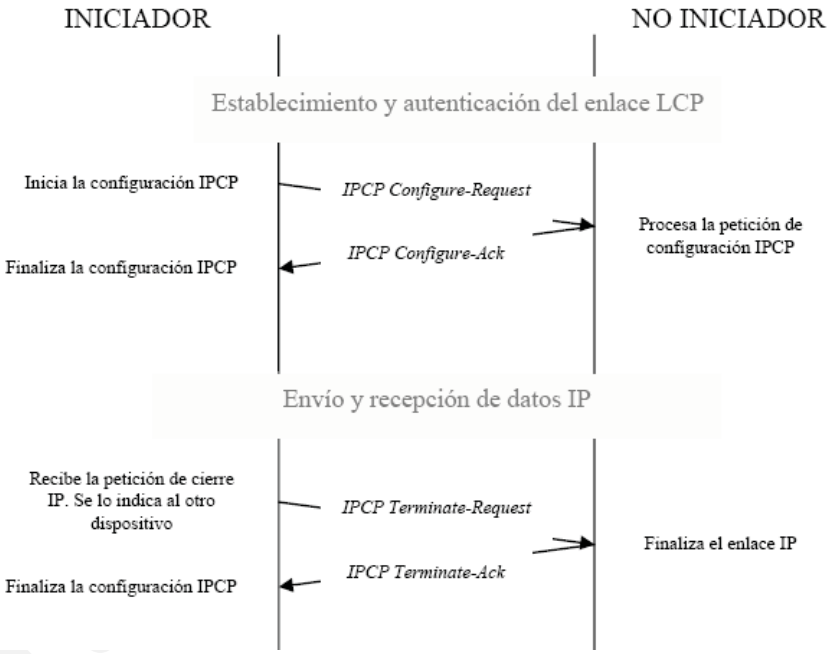
PPP. LCP.



Nº 497

Administración Avanzada de Redes TCP/IP

PPP. Protocolo NCP para IP. IPCP



Nº 498

PPP. Intercambio de mensajes en conexión GPRS.

```
Serial connection established.
using channel 10
Using interface ppp0
Connect: ppp0 <--> /dev/ttyACM0
sent [LCP ConfReq id=0x1 <asyncmap 0x0>]
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0>]
rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <auth pap> <magic0xa9e45> <pcomp> <accomp>]
sent [LCP ConfRej id=0x1 <magic 0xa9e45> <pcomp> <accomp>]
rcvd [LCP ConfReq id=0x2 <asyncmap 0x0> <auth pap>]
sent [LCP ConfAck id=0x2 <asyncmap 0x0> <auth pap>]
sent [LCP EchoReq id=0x0 magic=0x0]
sent [PAP AuthReq id=0x1 user="vodafone" password=<hidden>]
rcvd [LCP EchoRep id=0x0 magic=0x0]
rcvd [PAP AuthAck id=0x1]
PAP authentication succeeded
```

Nº 499

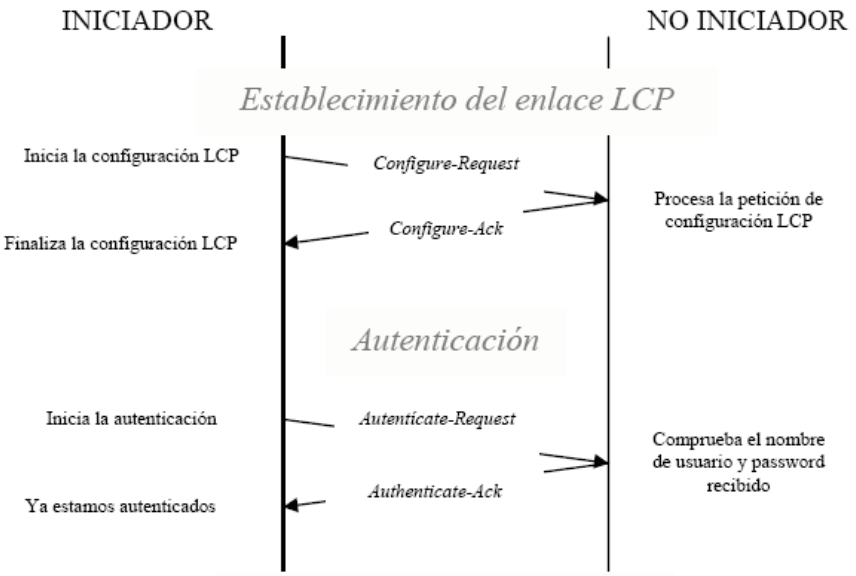
Administración Avanzada de Redes TCP/IP

PPP. Intercambio de mensajes en conexión GPRS.

```
sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <msdns3 0.0.0.0>]
sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <msdns3 0.0.0.0>]
rcvd [IPCP ConfNak id=0x1 <addr 212.166.151.190> <ms-dns1 212.73.32.3> <ms-dns3 212.73.32.67>]
sent [IPCP ConfReq id=0x2 <addr 212.166.151.190> <ms-dns1 212.73.32.3> <ms-dns3 212.73.32.67>]
rcvd [IPCP ConfAck id=0x2 <addr 212.166.151.190> <ms-dns1 212.73.32.3> <ms-dns3 212.73.32.67>]
rcvd [IPCP ConfReq id=0x3 <addr 192.168.100.101>]
sent [IPCP ConfAck id=0x3 <addr 192.168.100.101>]
not replacing default route to eth0 [158.49.113.5]
Cannot determine ethernet address for proxy ARP
local IP address 212.166.151.190
remote IP address 192.168.100.101
primary DNS address 212.73.32.3
secondary DNS address 212.73.32.67
secondary DNS address 212.73.32.67
Script /etc/ppp/ip-up started (pid 5735)
Script /etc/ppp/ip-up finished (pid 5735), status = 0x0
Terminating on signal 2.
Connect time 0.1 minutes.
Sent 0 bytes, received 0 bytes.
Script /etc/ppp/ip-down started (pid 5765)
sent [LCP TermReq id=0x2 "User request"]
rcvd [LCP TermAck id=0x2 "User request"]
Connection terminated.
Disconnecting...
```

Nº 500

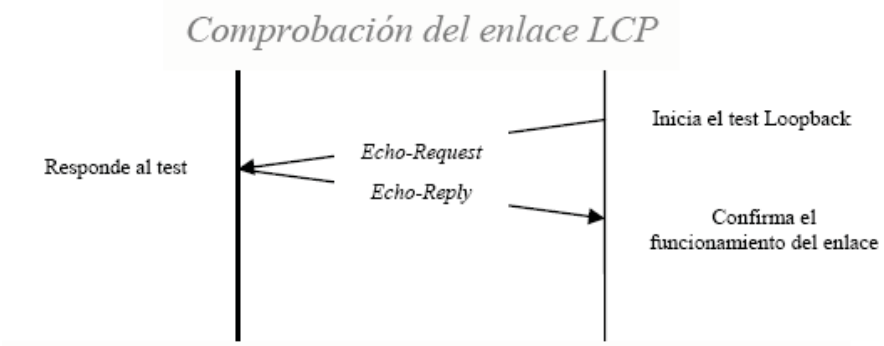
PPP



Nº 501

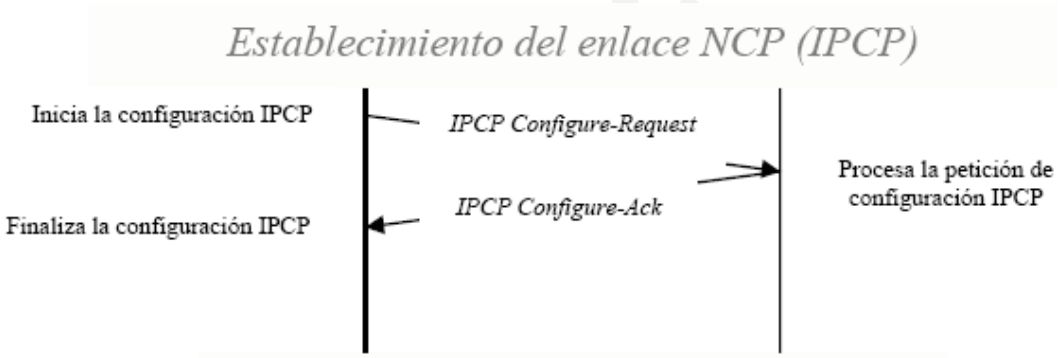
Administración Avanzada de Redes TCP/IP

PPP



Nº 502

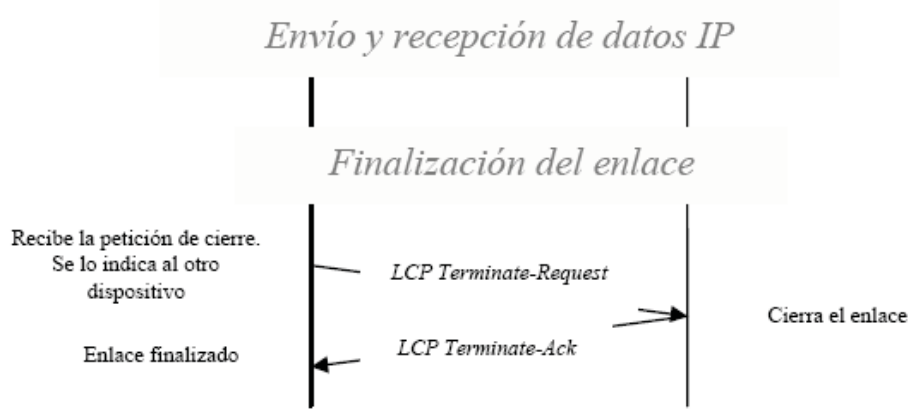
PPP



Nº 503

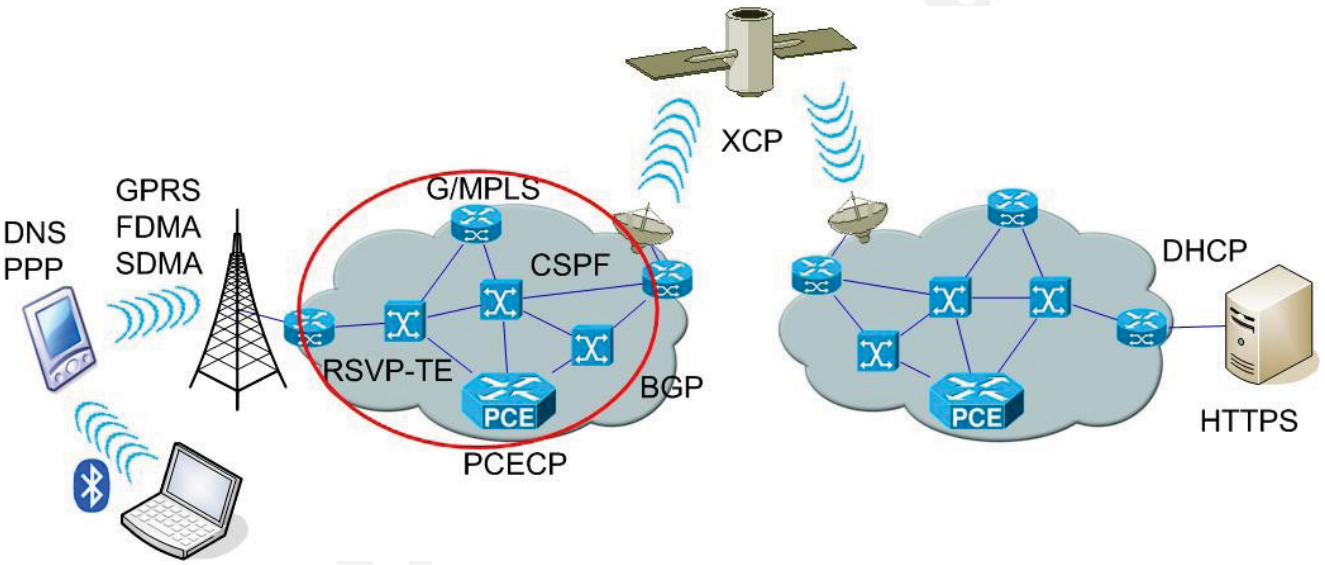
Administración Avanzada de Redes TCP/IP

PPP



Nº 504

Esquema de la conexión



Nº 505

Administración Avanzada de Redes TCP/IP

Miscelánea de protocolos: CSPF (I)

• En el caso de CSPF (*Constrained Shortest Path First*), la determinación de rutas no está diseñada para encontrar la mejor ruta hacia los demas nodos, sino sólo hasta el nodo final de un LSP.

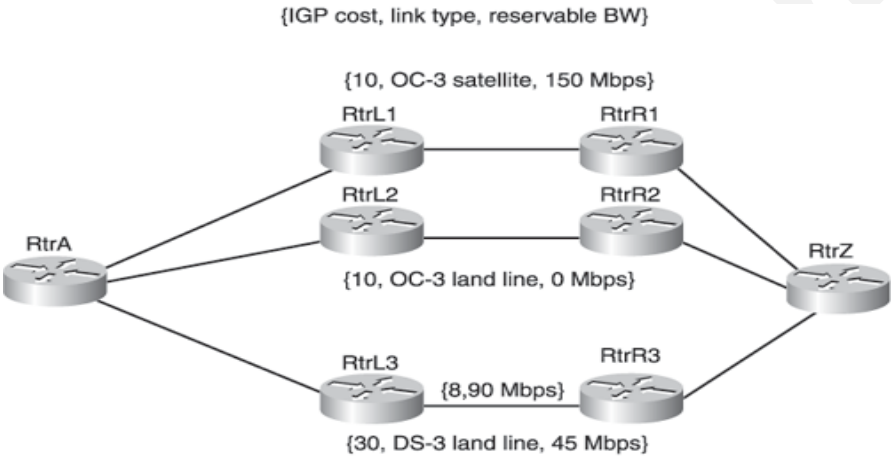
• El algoritmo se detendrá cuando el nodo destino forme parte de la ruta calculada. No se pre-calcularán más rutas de mínimo coste hacia el resto de nodos. Objetivo: conseguir un objeto *ERO* (*Explicit Route Object*), que es una ruta simple hacia un nodo particular.

• En lugar de emplear un valor simple de coste para cada enlace, también se podrán tener en cuenta otros costes o restricciones: Ancho de banda de enlace, peso administrativo, mínimo ancho de banda de ruta, mínima métrica IGP de una ruta, mínimo número de saltos, ...

• Se tendrá también la posibilidad de incluir o excluir ciertos nodos, permitiendo especificar un conjunto de nodos o enlaces que podrán ser utilizados o evitados en el cálculo de la ruta.

Nº 506

Miscelánea de protocolos: CSPF (II)



• ¿Es preferible una ruta con ancho de banda elevado pero alta latencia o una con menor latencia pero a costa de disponer de un menor ancho de banda?: Depende, si es un flujo de datos no le importará demasiado los retardos altos, si se trata de voz, no requerirá un elevado ancho de banda.

Miscelánea de protocolos: RSVP-TE (I)

• Después de que se haya obtenido el *ERO* óptimo con CSPF, dicha ruta se tiene que señalizar a través de la red, mediante el reparto salto a salto de etiquetas (también para hacer la correspondiente reserva de recursos).

• RSVP-TE (*Resource Reservation Protocol with Traffic Engineering*) se encargará de esto (RFC 3209). En el RFC 3473 se especifican las extensiones de RSVP-TE para señalizar caminos sobre GMPLS (*Generalized MPLS*).

• RSVP-TE tiene 3 funciones básicas: establecimiento y mantenimiento de rutas, cierre de rutas y señalización de errores.

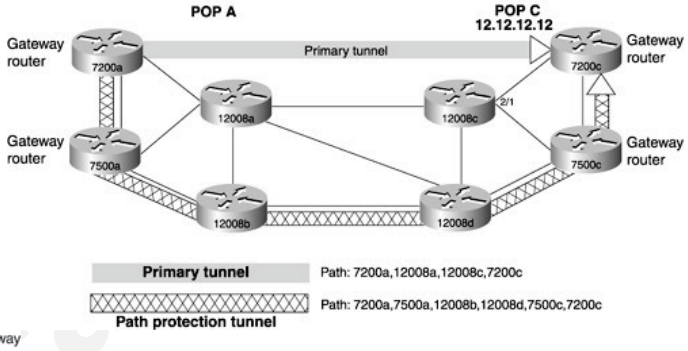
• RSVP-TE es un protocolo de tipo *soft-state*, es decir, necesita refrescar periodicamente su configuración. Por ejemplo, cada nodo necesita enviar mensajes *Path* periodicamente, de los que recibirá mensajes *Resv*. Si envía 4 mensajes Path sin recibir ningún *Resv*, considerará que el LSP y su reserva se han cancelado.

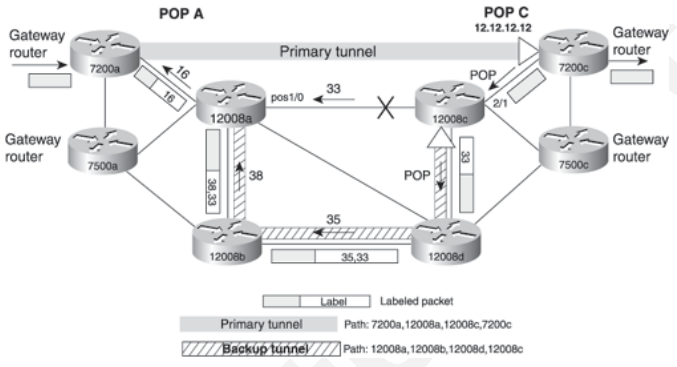
Miscelánea de protocolos: RSVP-TE (II)

Tipo de mensaje	Descripción
<Path>	Usado para establecer y mantener rutas y reservas de recursos.
<Resv>	Enviado en respuesta a un mensaje *Path* (confirmación de ruta y reservas).
<PathTear>	Análogo al mensaje *Path* pero para el cierre de la ruta y reservas.
<ResvTear>	Análogo al mensaje *Resv* pero para el cierre de la ruta y reservas.
<PathErr>	Enviado por un nodo que recibe un *Path* y encuentra algún problema.
<ResvErr>	Enviado por un nodo que recibe un *Resv* y encuentra algún problema.
<ResvConf>	Enviado (opcionamente) hacia el emisor de un *Resv* para confirmar la correcta configuración de la actual ruta LSP (y su reserva de recursos).
<ResvTearConf>	Mensaje propietario análogo al *ResvConf* usado para confirmar el cierre correcto de la actual ruta LSP (y su reserva de recursos).
<Hello>	Mecanismo de envío de *keepalives* entre nodos vecinos. Permite detectar problemas de conectividad entre nodos directamente conectados.

Miscelánea de protocolos: RSVP-TE (III)

- Protección extremo a extremo del túnel LSP: Se elige una ruta disjunta con respecto al LSP principal entre el LER de entrada y el de salida. La relación entre LSP principal y LSPs de respaldo es 1:1 ⇒escalabilidad limitada.





- Protección local de un enlace o nodo del túnel LSP: sólo cubre un segmento del LSP principal. Relación LSPs principal/respaldo es 1:N ⇒ mayor escalabilidad. En caso de fallo la conmutación al LSP de respaldo es más rápida. Funcionamiento basado en *label stacking*.

Miscelánea de protocolos: GMPLS (I)

• Generalized MPLS (GMPLS) extiende MPLS para proporcionar el *Plano de Control* (señalización y encaminamiento) a dispositivos que conmuten en base a paquete, tiempo, longitud de onda o fibra.

• Objetivo: simplificar las operaciones de reenvío y gestión de la red automatizando la creación de conexiones end-to-end, gestionando recursos disponibles en la red y aportando el nivel de QoS de las aplicaciones del futuro, con soporte, además, de redes ópticas.

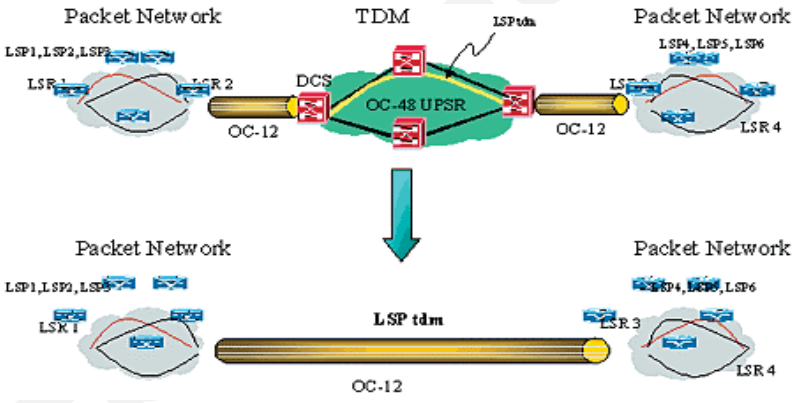
• LMP (*Link-Management Protocol*) es el protocolo para la gestión y mantenimiento de los planos PC y PR entre dos nodos vecinos (RFC 4204):

- Control-Channel Management: Negociado de los parámetros de enlace (por ejem. frecuencia de envío de mensajes keep-alive), asegurando al mismo tiempo la salud de los enlaces (protocolo Hello).
- Link-Connectivity Verification: Asegura la conectividad física entre vecinos intercambiando mensajes del tipo PING.
- Link-Property Correlation: Identificación de las propiedades de los enlaces a nodos adyacentes (como mecanismo de protección).
- Fault Isolation: capacidad de aislar uno o múltiples fallos en el dominio.

Miscelánea de protocolos: GMPLS (II)

• Para establecer un LSP entre dos nodos de un dominio GMPLS *(Generalized MPLS)*, otros LSPs de nivel inferior deben establecerse antes. Esto se logra enviando la solicitud de etiquetas hacia el destino, lo cual provoca la creación jerárquica de LSPs. Sólo cuando se establece un LSP de nivel inferior puede crearse el LSP de nivel inmediatamente superior.

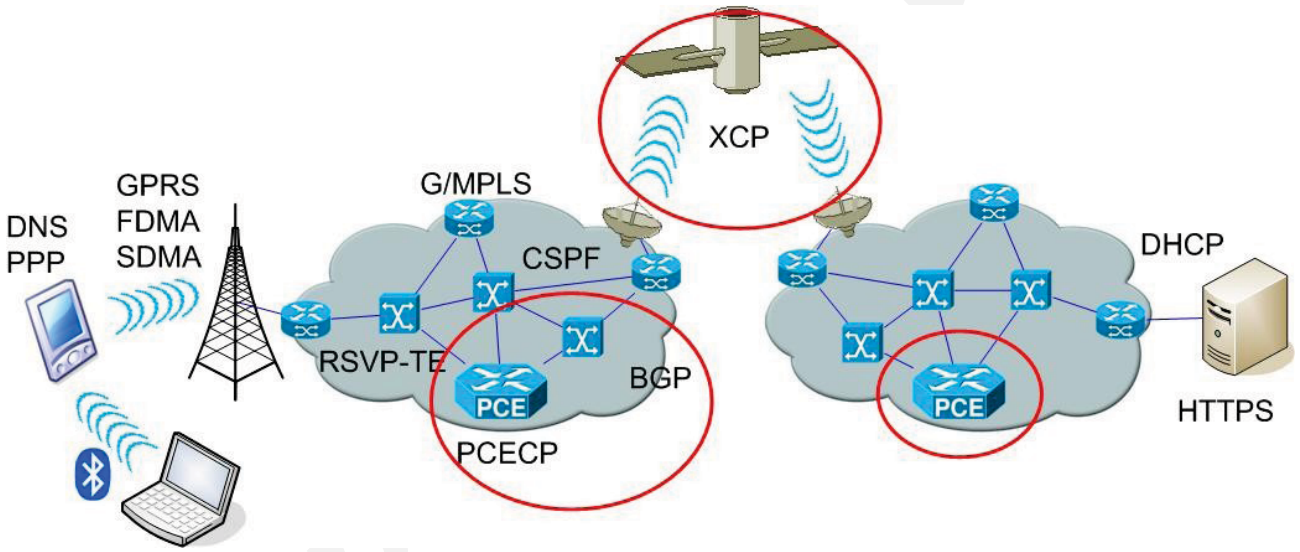
• Un FA–LSP (*Forwarding Adjacency-LSP*) es un LSP GMPLS que incluye otros LSPs. Es un enlace virtual con características *TE* propias y que puede procesarse como un enlace GMPLS.



Miscelánea de protocolos: MPλS

- Conmutación basada en longitudes de onda (colores) y no en etiquetas.
- Características de los conmutadores de paquetes ópticos:
  - Matriz de conmutación y buffers son ópticos.
  - Bit-rate independiente del payload.
  - Cabeceras procesadas electrónicamente todavía.
- Problemas por resolver en los buffers ópticos:
  - Son bobinas de fibra óptica (FO).
  - Aumentar la capacidad del buffer implica aumentar la cantidad de FO.
  - Son buffers poco eficientes: son de baja capacidad, pueden alterar el orden de los paquetes, pierden eficiencia si los paquetes son de tamaño variable o llegan asincronamete y, además, son memorias FIFO, no permiten acceso aleatorio.

Esquema de la conexión



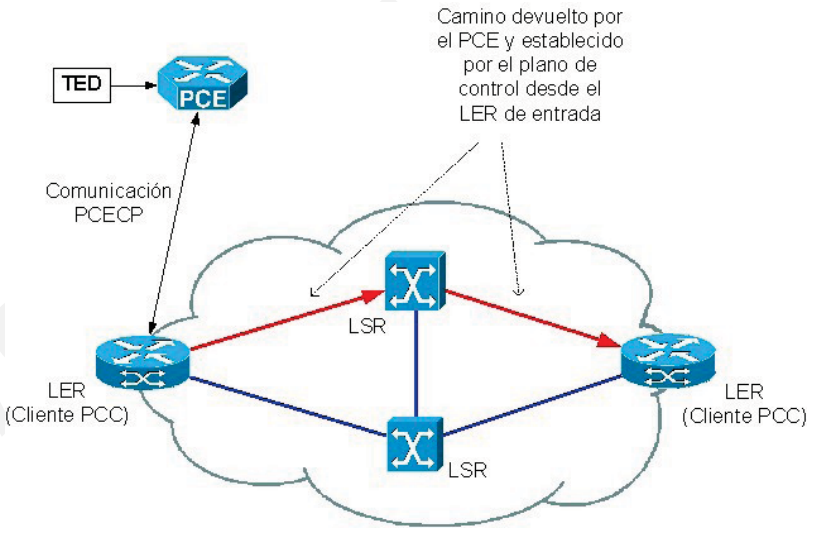
Miscelánea de protocolos: PCE (I)

- BGP es un protocolo de encaminamiento interdominio. Sin embargo, no es un protocolo adecuado para su funcionamiento conjunto con MPLS:
  - No tiene facilidades para aplicar ingeniería de tráfico.
  - No utiliza las métricas habituales en los protocolos de encaminamiento interior, sino políticas.
  - No sigue la misma filosofía de MPLS, sino de IP.
- Por ello, el IETF está desarrollando una arquitectura que permita el encaminamiento del tráfico interdominio para G/MPLS. La arquitectura PCE.
- PCE *(Path Computation Element)* pretende liberar a los nodos de una red MPLS y GMPL de la tarea del cálculo de caminos. Hoy en día, el cálculo de caminos es algo bastante complejo porque no solo se pretende que el tráfico llegue a su destino, sino que lo haga con seguridad, fiabilidad, garantías y optimizando los recursos de la red sobre la que fluye.

Miscelánea de protocolos: PCE (II)

- PCE involucra diversos elementos en la propia arquitectura:

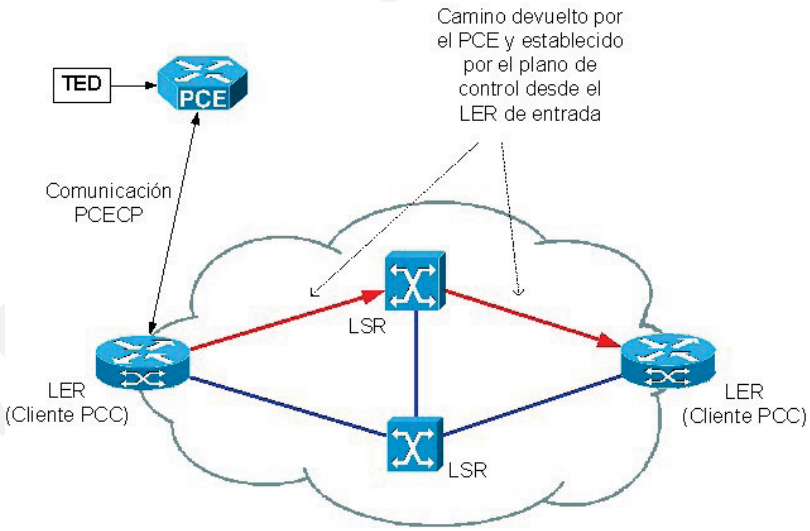
- **PCE:** elemento encargado de calcular caminos usando para ello restricciones y funciones objetivo.
- **TED:** base de datos de ingeniería de tráfico. Tiene datos sobre la topología.
- **PCC:** cliente. Solicita los servicios del PCE puesto que es quién requiere un camino con ciertas características.



Miscelánea de protocolos: PCE (III)

- PCE involucra diversos elementos en la propia arquitectura:

- **PCECP:** protocolo de comunicaciones entre el PCC y el PCE o entre PCE que colaboran para calcular un camino hacia el destino.

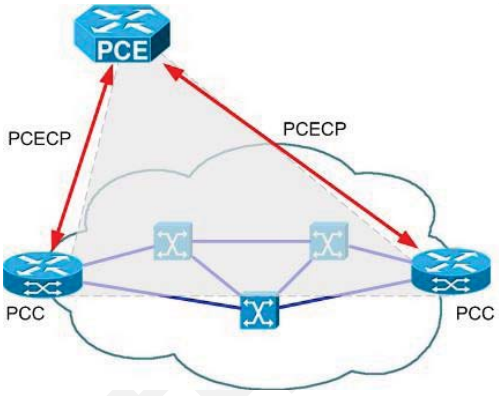


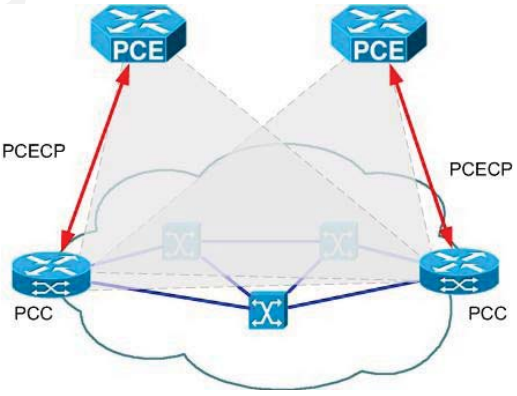
Nº 517

Administración Avanzada de Redes TCP/IP

Miscelánea de protocolos: PCE (IV)

- Puede haber:
  - Un solo PCE para calcular el camino completo.
  - Varios PCE que pueden calcular el camino completo (libera carga).
  - Varios PCE y cada uno puede calcular sólo un segmento de camino (PCE que colaboran).

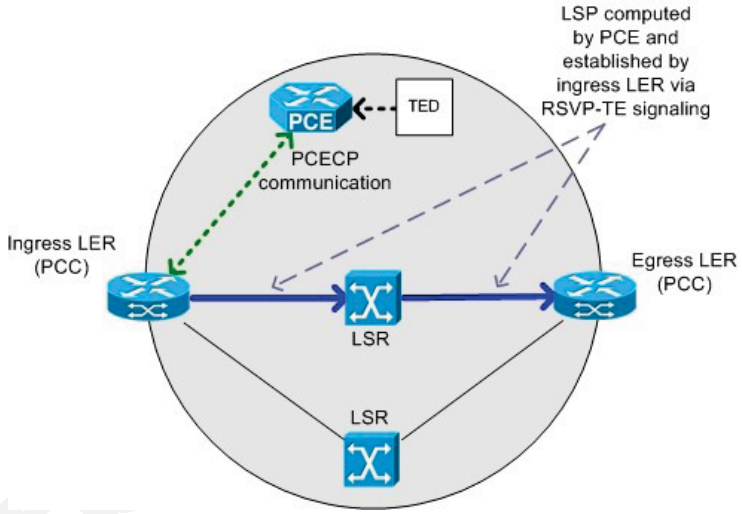




Nº 518

Miscelánea de protocolos: PCE (V)

- PCE está definido desde el principio para funcionar tanto en entornos intradominio...

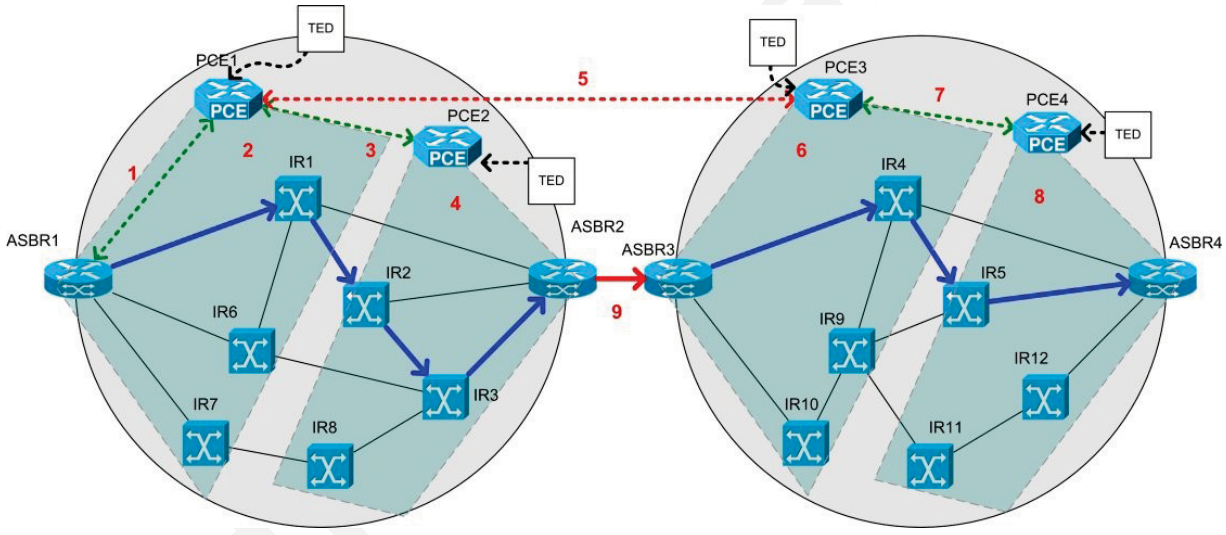


Nº 519

Administración Avanzada de Redes TCP/IP

Miscelánea de protocolos: PCE (VI)

- PCE está definido desde el principio para funcionar tanto en entornos intradominio... como en entornos interdominio.



Nº 520

Miscelánea de protocolos: PCE (y VII)

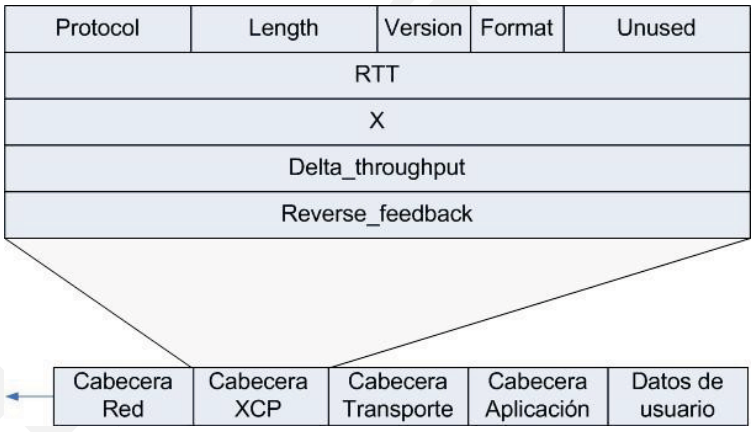
- La idea es simple:
  - Un PCC necesita calcular el camino para llegar al destino, con ciertas restricciones.
  - El PCC pide al PCE que calcule dicho camino ajustado a sus necesidades. Para ello utiliza PCECP *(Path Computation Element Communication Protocol)* y queda en espera...
  - El PCE calcula el camino y se lo devuelve al PCC vía PCECP.
  - El PCC establece el camino (PCE no establece, sólo calcula) mediante protocolos de señalización como RSVP-TE.
  - El tráfico comienza a fluir por el camino.
- La verdadera dificultad reside en el hecho de que probablemente un nodo PCE no sea capaz de calcular el camino completo por si mismo, sino que tenga que colaborar con otros. En este caso se desencadena un mecanismo para coordinar todo el proceso. El PCC no se entera; recibe el camino y punto.

Miscelánea de protocolos: XCP (I)

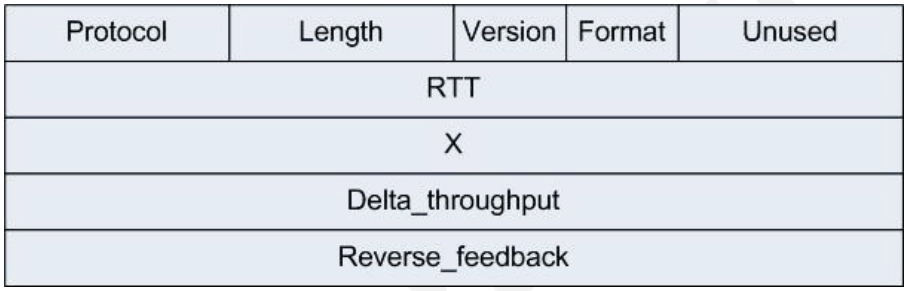
- ¿Qué es XCP?:
  - XCP *(Explicit Control Protocol)* es un protocolo en fase de desarrollo ideado para dotar a las comunicaciones actuales de un mecanismo de control de flujo encaminado a evitar congestiones en la red.
- Eso ya lo hace TCP, entonces... ¿Que hay de nuevo?
  - XCP funciona, en principio, con cualquier protocolo de transporte; y no siempre se usa TCP como protocolo de transporte.
  - TCP no permite a las redes actuales tener el rendimiento esperado; específicamente en redes con ancho de banda y latencias elevados (comunicaciones vía satélite, por ejemplo).
  - TCP tampoco permite sacar partido de forma correcta a redes de gran productividad.

Miscelánea de protocolos: XCP (II)

- ¿Cómo funciona XCP?:
  - XCP utiliza para su funcionamiento una cabecera de congestión asociada a cada paquete circulante. Además, requiere la colaboración de los elementos implicados: emisor, receptor y nodos intermedios.
  - La cabecera XCP se sitúa entre la de red y transporte de cada paquete.



Miscelánea de protocolos: XCP (III)



- **Protocol:** indica el protocolo que viene trás la cabecera XCP (TCP...).
- **Length:** longitud de la cabecera XCP.
- **Version:** versión del protocolo XCP. Actualmente, 2.
- **Format:** indica el formato de la cabecera, que puede ser *standard* o *minimal*.
- **Unused:** espacio no usado.

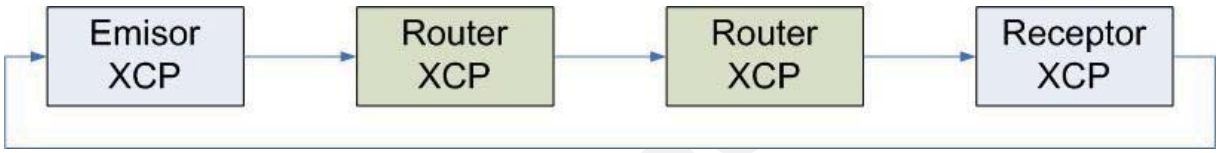
Miscelánea de protocolos: XCP (IV)

Protocol	Length	Version	Format	Unused
RTT				
X				
Delta_throughput				
Reverse_feedback				

- **RTT:** *Round Trip Time* estimado por el emisor de tráfico.
- **X:** tiempo entre paquetes estimado por el emisor.
- **Delta_throughput:** indica la cantidad con la que desea el emisor que se le aumente o disminuya la productividad aconsejada.
- **Reverse_feedback:** mismo valor que *Delta_throughput*, copiado a este campo y enviado por el receptor en paquetes de tipo ACK.

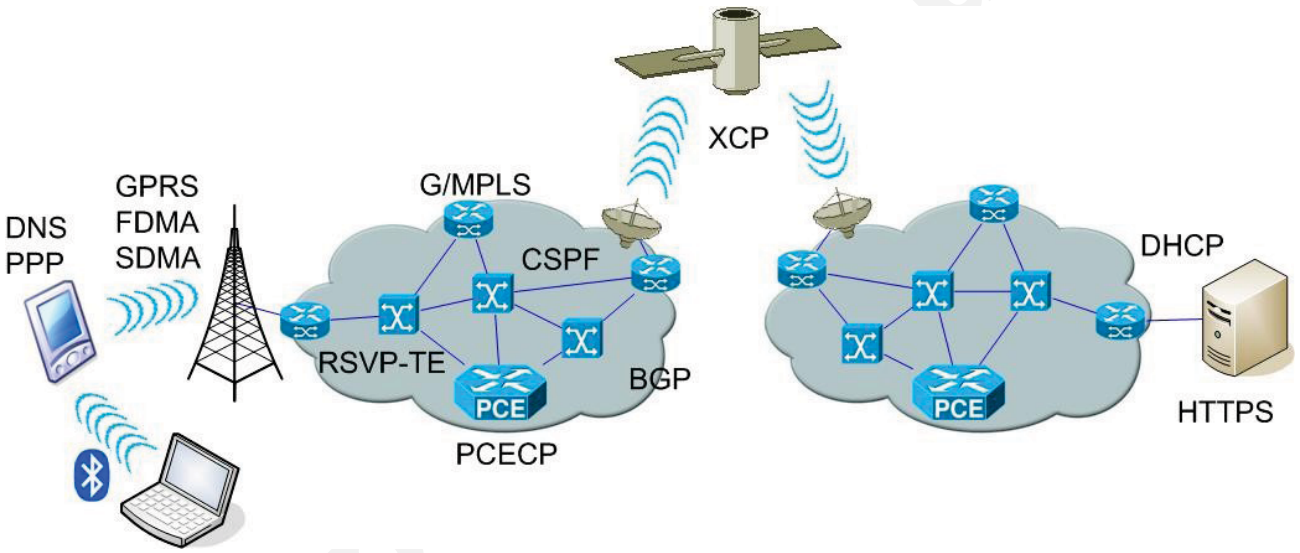
Miscelánea de protocolos: XCP (y V)

- ¿Cómo funciona XCP?:



- El emisor envía paquetes al receptor con su cabecera XCP correspondiente.
- En la cabecera el emisor indica el *throughput* deseado y con el que en principio emitirá tráfico.
- Los *routers* XCP intermedios modifican la cabecera XCP, aumentando o disminuyendo el valor de *Delta_throughput* según su nivel de congestión.
- Al final, el receptor copia *Delta_throughput* a *Reverse_feedback* y envía un ACK al origen con esta información.
- El emisor usa el *Reverse_feedback* para ajustar su tasa de envío y no congestionar la red.

Esquema de la conexión



Nº 527

Administración Avanzada de Redes TCP/IP

Administración y mantenimiento

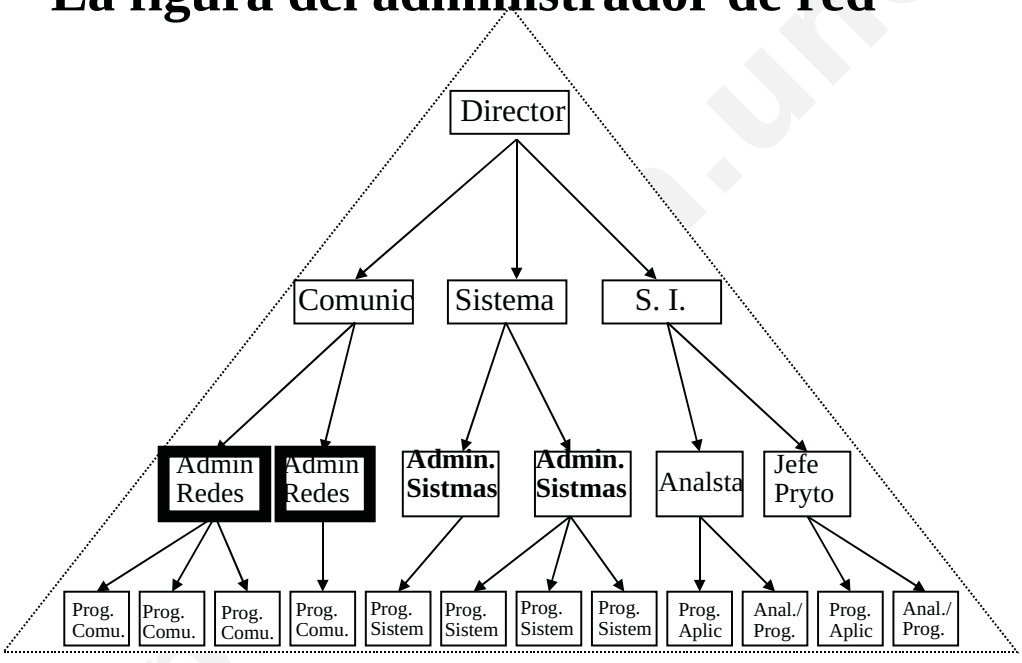
Nº 528

La figura del administrador de red

- Administrador de red, Especialista de red, Analista de red.
- Administrador de red (para redes) equivalente a Administrador de sistemas (para sistemas): Mantiene hardware y software que forma parte de la red:
  - Despliegue, configuración, mantenimiento y monitorización de equipamiento de red: switches, routers, firewalls, etc.
  - Asignación de direcciones (no necesariamente de forma manual)
  - Despliegue de protocolos de routing. Configuración de tablas de routing
  - Servicios de directorio
  - Configuración de elementos de red en equipos (drivers, parámetros). ¿Qué equipos?
    - Ordenadores personales
    - Impresoras en red
    - Servidores de archivos, gateways VPN, sistemas IDS, etc. (¡A veces no sólo red!)

Administración Avanzada de Redes TCP/IP

La figura del administrador de red



Los límites de la red

- Los límites de una red se establecen por dispositivos como:
  - Routers
  - Switches
  - Hubs
  - Bridges
  - Multi-homed gateways
  - ...
- Los segmentos pueden clasificarse de la siguiente forma:
  - Redes públicas.
  - Redes semi-públicas
  - Redes privadas

Elementos de red (I)

- Las principales categorías de equipación de red incluyen concentradores, conmutadores, multiplexores, *bridges* y *routers*.
- Antes de que los *bridges* y los *routers* estuvieran disponibles en el mercado, sus funciones las realizaban equipos *mainframe*.
- Ahora, las funciones de *bridging*, *routing* y *switching* se integran habitualmente en un único dispositivo.
- Cada una de estas tecnologías de hardware ofrece ventajas y desventajas específicas en función de las necesidades respecto a aplicaciones de usuario, protocolos, direccionamiento y transporte de datos.

Elementos de red (II) - Repetidores

- Los repetidores son dispositivos que proporcionan una extensión física de distancia.
- Utilizan regeneración de señal sobre circuitos punto a punto.
- Proporciona entonces una extensión de distancia entre dispositivos de red, pero también proporciona aislamiento eléctrico si ocurren problemas.
- Son dispositivos con poca “inteligencia”.
- Completamente transparentes para todo el contenido que circule por la red.
- Como desventajas:
  - Posible congestión en la red debido al *overhead* de repetición.
  - *Jitter* debido al retardo de la señal.
- Los repetidores son el componente central de los concentradores.
- Se encuentran únicamente en la capa física.

Administración Avanzada de Redes TCP/IP

Elementos de red (III) - Concentradores

- Son elementos que conectan:
  - Varios segmentos LAN.
  - Estaciones de trabajo.
- Los concentradores se han clasificado en cuatro generaciones:
  - Primera generación:
    - Apareció en 1984
    - Actúa como repetidor para un único tipo de conectividad LAN.
  - Segunda generación:
    - Proporciona la misma arquitectura en bus que la primera, pero puede interconectar diferentes arquitecturas LAN sobre múltiples puertos (e.j. Ethernet y Token Ring).
    - Posteriormente se añadieron características de gestión y configuración tanto local como remota.

Elementos de red (IV) - Concentradores

- (continúa)
  - Tercera generación:
    - Proporcionan varios buses para lograr una conectividad similar a los de segunda generación, pero también añaden funciones de *bridging* y *routing*.
    - El rango de medios físicos soportados es mucho mayor.
    - La arquitectura del bus puede ofrecer varios buses multimegabit.
    - Incorporan características de gestión de red.
    - Incorporan algún tipo de protocolo de gestión de red, como SNMP.
    - Algunos incorporan capacidades de *trunking* propietarias.
  - Cuarta generación:
    - Aparecen al final de los 90.
    - También se denominan *conmutadores LAN* o de nivel 2.
    - Ofrecen las capacidades de la generación anterior añadiendo conmutación en la capa MAC, *bridging* transparente e interfaces de *trunking* estándar.

Elementos de red (V) - *Bridges*

- Los *bridges* proporcionan conectividad entre LAN de arquitecturas idénticas o “similares”.
- Forman una de las conexiones más simples entre LAN y WAN.
- Un *bridge* utiliza una capacidad de proceso mínimo y por ello es un modo barato de interconectar redes.
- Los *bridges* deben ser transparentes al protocolo, por lo que no proporcionan funcionalidad de:
  - control de flujo,
  - conmutación,
  - direccionamiento
  - tampoco reconocen protocolos de niveles más altos: sólo utilizan las capas físicas y de enlace (OSI) y soportan las capas LLC y MAC (LAN).

Elementos de red (VI) - *Bridges*

- Los *bridges* tan sólo pasan tráfico desde un segmento de red hasta otro.
- Para ello se basan en la dirección MAC de destino de la trama que va a ser pasada.
- Si la dirección de destino de la trama recibida por el *bridge* no es una dirección local, el *bridge* supone que va destinada a otra LAN y por ello reenvía la trama al siguiente interfaz de red.
- Los *bridges* pueden utilizar:
  - una tabla de encaminamiento estática
  - esquemas de aprendizaje de encaminamiento dinámico; los bridges pueden "aprender" la red mediante la utilización de protocolos inteligentes de *bridging* y *routing*.
- Además también pueden filtrar datos.
- Sin embargo, no deben utilizarse en diseños de red que necesiten:
  - Soporte de múltiples protocolos.
  - Redes dinámicas de cambios frecuentes.
  - Redes mayores de 50 nodos.

Elementos de red (VII) - *Routers*

- Los *routers* utilizan nivel físico, enlace y red para proporcionar funcionalidad de direccionamiento y conmutación.
- Disponen de al menos dos interfaces de red y pueden interpretar varios protocolos de red y esquemas de direccionamiento.
- Los *routers* "comprenden" toda la red, no sólo los dispositivos conectados localmente a ellos, y encaminan los paquetes basándose en varios factores a la hora de determinar el camino mejor.
- La funcionalidad principal de un *router* reside en los niveles de enlace y de red pero emplean, obviamente, el nivel físico.
- Las aplicaciones de los extremos de la comunicación no tienen porqué utilizar los mismos protocolos de hasta nivel 3, pero deben utilizar los mismos protocolos a partir del nivel 4.
- Los *routers* utilizan protocolos de interconexión de red que les sirven para conseguir cierta IA, más correctamente denominado "conocimiento dinámico" de la red.

Elementos de red (VIII) - *Routers*

- Los protocolos de *routing* pueden descubrir cambios en la topología de red y establecer re-encaminamientos basándose en tablas de encaminamiento dinámicas.
- Los *router* también pueden limitar el número de saltos (*hop-count*) gracias a sus protocolos de *routing*.
- Utilizan esquemas de direccionamiento de hasta 4 Bytes en una red lógica. Excepciones.
- Soportan grandes tamaño de paquete (FR ~ 8000 Bytes).
- Las velocidades de los buses internos son del orden de Gbps.
- Además pueden realizar todas estas funciones mediante el uso de *software*: revisiones y actualizaciones.
- El encaminamiento puede basarse en:
  - Menor coste.
  - Retardo mínimo.
  - Distancia mínima.
  - Menor congestión.

Elementos de red (IX) - *Routers*

- Los *routers* pueden determinar automáticamente las direcciones de los dispositivos conectados a una red de *routers*. (*Interior Routing Protocol*)
- Los *routers* también pueden determinar automáticamente las direcciones de los dispositivos conectados a una red de redes. (*Exterior Routing Protocol*).
- En cualquier caso, las estrategias de encaminamiento estático (configurado manualmente por un operador) son comunes: la segmentación de subredes es el caso más claro.
- Los *routers* pueden manejar tanto servicios de red orientados a conexión como no orientados a conexión.
- También pueden interconectar diferentes medios físicos y protocolos de enlace realizando conversiones.
- Monitorizan constantemente el estado de los enlaces:
  - Que interconectan los *routers* en una red.
  - Que están conectados a otras redes.
- Las interfaces pueden ser LAN, MAN o WAN, y el encaminamiento puede realizarse entre cualquiera de ellas.
- Son gestionables mediante el uso de uno o varios de los siguientes protocolos: SNMP, CMIP, NetView, LAN Net Manager, DEC MOP, Windows PC Configuration Builder.

Elementos de red (X) – *Routers vs. Bridges*

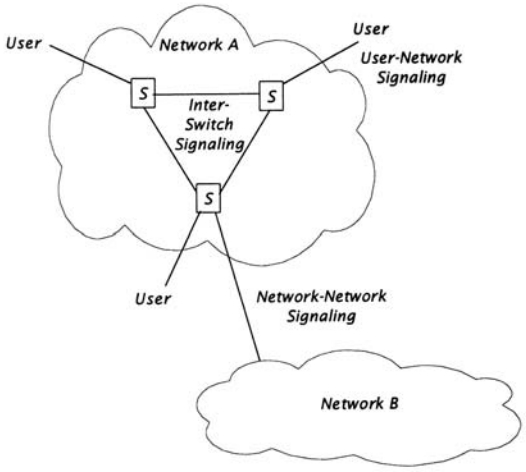
Funcionalidad	*Bridging*	*Routing*
Fuentes de datos	Un origen y un destino	Varios orígenes y destinos
Direccionamiento de red	No	Sí
Manejo de paquetes	Paso transparente	Interpretación del paquete
Reenvío de paquetes	Hacia fuera	Con destino específico
Inteligencia global de red	Ninguna	Conocimiento del estado de todos los dispositivos
Esquemas de prioridad	No	Sí
Seguridad	Basada en el aislamiento	Basada en el protocolo de encaminamiento

Elementos de red (XI) - *Brouters*

- El término *brouter* viene de una unión entre *bridge* y *router*.
- Los *brouter* realizan las funciones tanto de *bridges* como de *routers*.
- Seleccionan una función u otra en función del protocolo: realizan *bridging* para unos protocolos y *routing* para otros.
- Algunos protocolos no pueden utilizar *routing* (e.j.: NetBIOS o DEC LAT), así que el *brouter* actúa como *bridge* para ellos.
- El *routing* realizado por los *brouter* es transparente tanto para los protocolos del nivel de red como para las estaciones y se realiza mediante direcciones MAC.
- Los *brouter* no interpretan, por tanto, las direcciones de red.

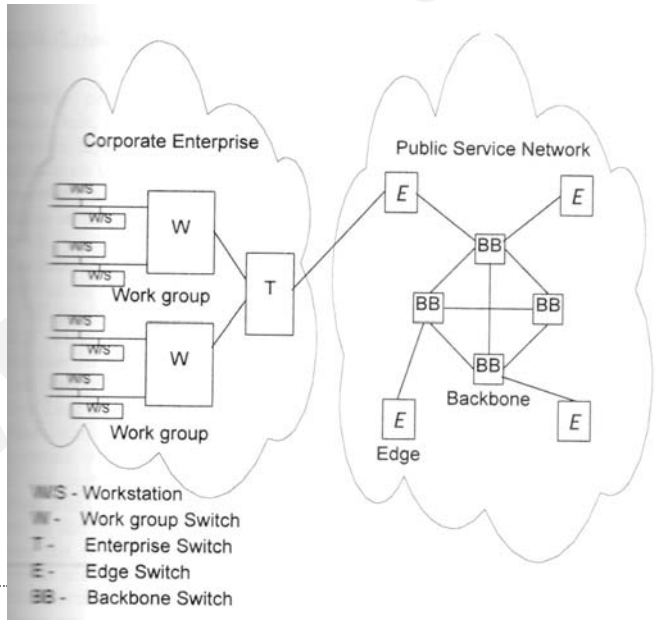
Elementos de red (XII) - Switches

- Los *switches* son dispositivos orientados a conexión.
- Los usuarios interaccionan con los *switches*, enviando la información para el requerimiento de conexiones, mediante un protocolo de señalización UNI.
- Entre *switches* se puede utilizar un protocolo propietario, pero en interconexión de redes mediante *switches* es necesario utilizar un protocolo de señalización NNI.
- Las funciones de los protocolos de señalización pueden ser emuladas por protocolos de gestión de red



Elementos de red (XIII) - Switches

- Existen cuatro clases generales de *switches*:
  - *Workgroup*
  - *Enterprise*
  - *Edge*
  - *Carrier Backbone*



Elementos de red (XIV) - Switches

- Atendiendo al RM-OSI, ¿en qué capas operan los *switches*?
- Diferenciamos dos tipos:
  - Nivel 2 (LAN switches).
    - Operan generalmente en el nivel MAC.
  - Híbridos niveles 2 y 3.
    - Se utilizan cuando se realiza algún tipo de conmutación basado en paquetes, tramas o celdas, como en el encaminamiento IP o la conmutación ATM.
    - Ejemplo: el situar en los *switches* el encaminamiento ATM permite proporcionar mejor QoS utilizando protocolos específicos de ATM.
      - Desventaja: mantenimiento de los VC.
  - ¿Otros?

Elementos de red (XV) - Multihomed Gateways

- Proporcionan el mismo nivel de conectividad que el proporcionado por *bridges* y *routers*.
- Además, ofrecen funcionalidad de conectividad y conversión entre protocolos ubicados en cualquiera de los 7 niveles de OSI.
- Los *gateways* dependen entonces de la aplicación y debido a las conversiones entre protocolos (generalmente complejas) son más lentos que *bridges* y *routers*.
- Los *gateways* generalmente residen en *workstations*, *servers*, *minicomputers* o *mainframes*.
- Son, por tanto, considerablemente más caras que *bridges* o *routers*.
- A pesar de que pueden convertirse en un punto de congestión en situaciones de picos de tráfico, los *gateways* proporcionan un modo de tratar con protocolos dispares.
- ¿Multihomed?

Elementos de red (XVI) - Proxies

- Un *proxy* es un servidor que se ubica entre una aplicación cliente y un servidor real.
- Intercepta todas las peticiones al servidor real y:
  - Determina si la petición debe atenderse (control de acceso).
  - Determina si la petición debe retrasarse para conceder mayor prioridad a otras.
  - Determina si la petición puede atenderse sin acceder al servidor real (caché).
  - Determina si la respuesta debe aceptarse (virus, malware, etc.).
  - Etc.
- Normalmente el proxy no es transparente al cliente y debe configurarse o bien la propia aplicación o bien el sistema operativo.

Elementos de red (XVII) - Proxies

- Un servidor proxy tiene tres funciones principales:
  - Conectividad.
  - Mejorar el rendimiento.
  - Filtrado de peticiones (y/o respuestas)
- Aunque también sirve para:
  - Políticas de prioridad.
  - Anonimizar accesos.
  - ...

Elementos de red (XVIII) - Firewalls

- Son dispositivos configurados para permitir, denegar o actuar como proxy ante el tráfico que pretende atravesar una red.
- Establece distintos niveles de confianza en el acceso a distintas redes. Ejemplos de zonas, de menor a mayor confianza:
  - Zona de Internet.
  - Zona DMZ (DeMilitarized Zone), también denominada “red perimetral”.
  - Zona Interna.
- Si el *firewall* no está correctamente configurado, se vuelve poco útil.

Elementos de red (XIX) - Firewalls

- Una configuración correcta de un *firewall* requiere de un exhaustivo estudio de las necesidades de conectividad de la organización donde se ubica.
- Los procedimientos estándar de seguridad dictan una política *default-deny*, para la que las únicas conexiones que se permiten son las que se han indicado de forma explícita.
- Sin embargo, muchas organizaciones no hacen este estudio, y acaban implantando una política *default-allow*, en la que las únicas conexiones que se deniegan son las que se han indicado de forma explícita.

Elementos de red (XX) - Firewalls

- 1ª Generación: *Packet Filter*.
  - Actúan inspeccionando los paquetes.
  - Si se encuentra una correspondencia con el conjunto de reglas, el filtro de paquetes **descartará** o **rechazará** el paquete.
  - Este tipo de filtro de paquetes no puede determinar si un paquete pertenece a un determinado flujo.
  - Problemas con protocolos que abren conexiones sobre puertos no conocidos (well-known).
    - FTP no pasivo (comando PASV).
    - Versión anterior del protocolo de MSN.
    - Xwindow.
    - ...

Elementos de red (XXI) - Firewalls

- 2ª Generación: *Stateful Filter*.
  - Mantiene un registro de todas las conexiones establecidas.
  - Puede determinar si un paquete pertenece al establecimiento de una conexión, o a una conexión previamente establecida.
  - Todavía existe un conjunto estático de reglas de filtrado.
  - Pero el criterio de establecimiento de conexiones puede utilizarse para determinar si un paquete debe ser filtrado o no.
  - Este tipo de firewall puede ayudar a prevenir ciertos tipos de ataques como DoS ó SYN flood.

Elementos de red (XXII) - Firewalls

- 3ª Generación: *Application Filter*.
  - También llamadas *proxy-based firewalls*.
  - Inspeccionan el *payload* de cada paquete.
  - Tratan de determinar si pertenecen a algún protocolo de aplicación conocido
  - Aunque se esté transmitiendo sobre un puerto no estándar.
  - O si se está transmitiendo de alguna forma dañina.
  - ¿Algún ejemplo?

Segmentación e Interconexión de Redes (I)

- Algunos motivos por los que una organización puede tener varias LAN:
  - Diferentes metas en diferentes departamentos: diferentes tecnologías de red.
  - Distribución geográfica en varios edificios.
  - Necesidad de división de una LAN en varias para distribuir la carga y las *broadcast storms*.
  - Distancia física excesiva entre las máquinas más distantes.
  - Fiabilidad: en una sola LAN, un *host* defectuoso o malicioso puede echar a perder toda la red.
  - Seguridad: no siempre es adecuado que la información se difunda a todos los equipos conectados a la red.

Segmentación e Interconexión de Redes (II)

- Si existen varias LAN, o existe una que se acaba segmentando, tarde o temprano será necesario interconectarlas:
  - Mecanismos de *bridging*.
  - Mecanismos de *routing*.
  - Mecanismos *brouting*.
- Desventajas
- ¿Y si no se realiza una segmentación física?

LAN Virtuales: VLAN

- Método de crear redes lógicas independientes sobre una misma red física.
- Para:
  - Reducir el dominio de broadcast.
  - ¿También el dominio de colisión?
  - Ayudar a la administración de la red, separando segmentos lógicos de una red que no deberían compartir datos utilizando LAN (pero sí utilizando *routing*)
- Consiste en una red de equipos que se comporta como si estuvieran conectados a la misma LAN.
- Pueden configurarse mediante *software* sin necesidad de reconfiguración *hardware*: gran flexibilidad.
- ¿Movilidad?

VLANs: ventajas

- Incrementan el número de dominios de broadcast, reduciendo su tamaño. Esto reduce el tráfico de red e incrementa la seguridad.
- Reducen el esfuerzo de gestión para crear subredes.
- Reducen los requerimientos de hardware, ya que se pueden separar las redes de forma lógica en lugar que de forma física.
- Incrementan el control sobre tipos de tráfico distintos.
- Sirven para crear varios *switches* lógicos sobre un *switch* físico

Nº 557