UTN-FRBA-Dto.Sistemas
Redes de Información

Unidad 5: Protocolos TCP/IP

Clase 1: Introducción y capa 3

Fuentes: Stallings, cap. 18 y 20-Comer, vol.1 y otras

Versión: 1

Introducción: Historia de Internet

- 1965: primeros ensayos en el MIT
- 1969: primer enlace entre computadoras
- El Dto. de Defensa forma ARPANET (*Advanced Research Projects Agency Network*)
- 1984: la red se divide en ARPANET y MILNET (militar)
- 1985: se incorpora la red de la NSF (*National Science Foundation*)
- 1992: se forma la ANSNET y la estructura de soporte actual
- 1995: se forma la *www* con aplicaciones comerciales

Operadores de Internet

- ISP (*Internet Service Provider*): empresas que conectan un router a Internet y ofrecen conectividad a los usuarios
- POP (*Point of Presence*): lugar donde el ISP ofrece el servicio
- NAP (*Network Acces Point*): interconexión entre los ISP
- NSP (*Network Service Provider*): realiza la conexión entre ISP y NAP

Asignación de direcciones

- Los usuarios obtienen las direcciones IP por los ISP
- Los ISP las obtienen de:
  - —LIR (Local Internet Registry)
  - —NIR (National Internet Registry)
  - —RIR (Regional Internet Registry).
- Estos últimos están divididos por región:
  - —America y parte de Africa: ARIN (American Registry for Internet Number).
  - —America Latina y el Caribe: LACNIC
  - —Argentina: NIC Argentina

- Las direcciones y dominios de la red son gestionadas por la *Internet Corporation for Assigned Names and Numbers* (ICANN)
- Hoy el desarrollo de los protocolos para la www los hace el *Word Wide Web Consortium* (WWWC)
- Futuro de Internet:
  - — Enlaces de gran capacidad
  - — Nuevo direccionamiento
  - — Incorporación de equipos móviles
  - — Mayor seguridad
- El gran desarrollo de Internet fue posible por el uso extendido de los protocolos TCP/IP

Historia de TCP/IP

- Protocolos propuestos en 1974 por Cerf y Kahn
- Ensayados en campo en 1978
- Adoptados por ARPANET en 1980 y por el Dto. de Defensa en 1983
- Los protocolos TCP/IP fueron originalmente diseñados por la *Internet Architecture Board*, (IAB), foro de investigadores que fue absorbido por la *Internet Society* (ISOC)
- Hoy son mantenidos por la *Internet Engineering Task Force* (IETF) con grupos de trabajo de investigadores voluntarios

Documentación

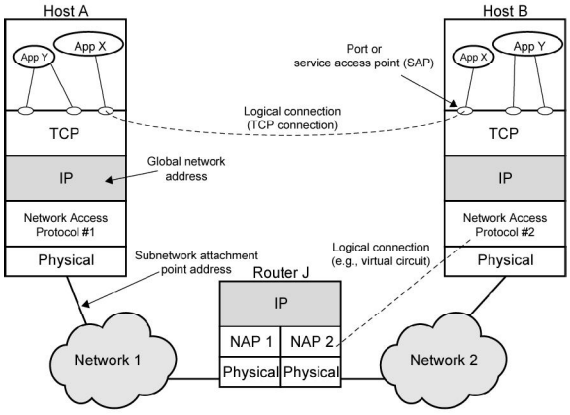
- Los protocolos TCP/IP están documentados en los RFC (*Request for Comment*), que incluyen borradores, propuestas, normas e instructivos
- El índice actualizado es el RFC 3600
- Los documentos en formato texto están disponibles en la red en el sitio:

  http://www.ietf.org

Ventajas de TCP/IP

- Es independiente del hardware y de los sistemas operativos (fueron desarrollados en Unix).
- No se encuentra afectado por la tecnología de los enlaces de datos.
- Soporta alta tasa de error de la red.
- Tiene capacidad de encaminamiento adaptivo.
- Genera redes "planas" en las cuales el alta o baja de los nodos no afecta al resto de las redes.
- Documentación disponible gratis

Concepto TCP/IP



Funcionamiento de la red

- Se desea intercambiar datos independientemente del hardware y software
- Todas las redes tienden a la interconexión a Internet
- La interconexión entre redes se hace mediante un *router*
- Los datos que salen de la computadora origen circulan por los router en forma de paquetes hasta llegar a la computadora destino
- Los routers toman decisiones en función de la dirección de la red destino (no de la computadora destino)
- El usuario visualiza la red como una nube a la que se conectan las computadoras de las aplicaciones (host)

Direccionamiento

- Los paquetes en la red buscan el destino identificado por su dirección física
- Cada tecnología tiene su modo de direccionamiento
- El direccionamiento puede ser
  - **Estático**: establecido por el fabricante
  - **Configurable**: establecido manualmente por el usuario
  - **Dinámico**: establecido automáticamente por el software

Tipos de redes

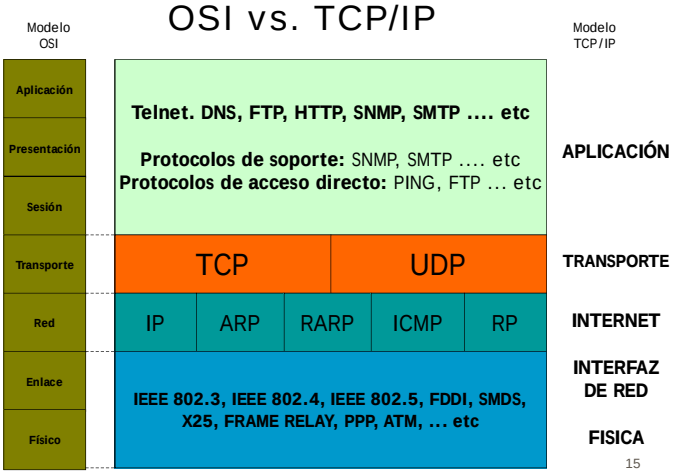
- Las redes orientadas a la conexión:
  - Operan por conmutación de circuitos
  - Deben establecer un circuito al comenzar
  - Trasmiten datos por el circuito armado
  - Liberan el circuito al terminar
  - Garantizan un ancho de banda
- Las redes no orientadas a la conexión
  - Operan enviando los datos divididos en paquetes
  - Los paquetes tiene distintos tamaños
  - Circulan por caminos distintos con identificación del destino

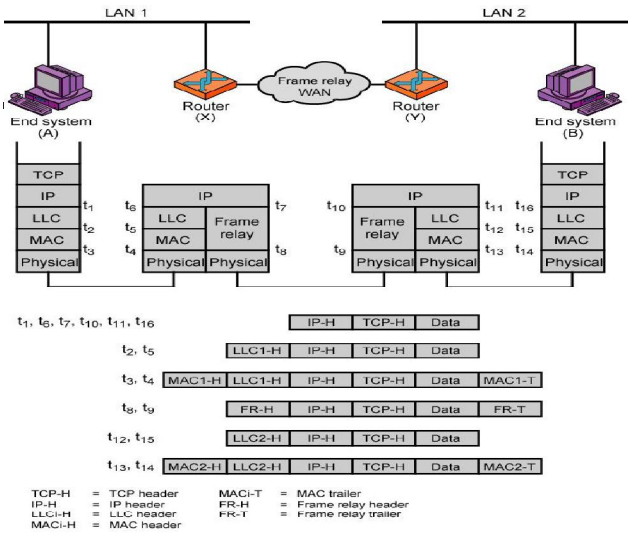
Arquitectura TCP/IP

- Los múltiples problemas de la comunicación de datos entre dos equipos se analizan con una estructura de capas
- Cada capa realiza una función e interactúa con las adyacentes
- El modelo ISO tiene 7 capas
- El modelo TCP/IP tiene cinco capas
  - Física
  - Interfaz de enlace
  - Red
  - Transporte
  - Aplicación

- En el encabezamiento de cada capa el trasmisor indica el protocolo que genera los datos
- En el receptor, esa capa entrega los datos al protocolo que corresponde
- Este proceso se llama multiplexado/demultiplexado

OSI vs. TCP/IP





Capas 1 y 2

- Son dependientes de la tecnología
- La capa 3 unifica la operación hacia arriba
- Para LAN: redes 802.3
- Para enlaces serie: protocolos SLIP y PPP (*Point to point protocol*) RFC 1661
  - Ambos permiten enlaces fijos y conmutados por red telefónica
  - PPP tiene direcciones y control de errores
  - Capa 2 con tramas HDLC y control de enlace
- Cablemodem
  - FDM en bandas asimétricas
  - Protocolo ATM en RX y 802.3 en Tx
- X.25 (hasta 64Kbps) o Frame Relay (hasta 2 Mbps)
- ATM: tiene un modo de emulación de LAN
- SDH: usan IP/PPP para llenar contenedores virtuales

Capa 3: Internet Protocol (IP)

- Provee un servicio de entrega de paquetes sin conexión
- Hay tres temas a resolver
  - Tipo de direccionamiento
  - Formato de datagrama
  - Ruteo de paquetes
- Formato de datagrama: a los datos de la capa superior se agrega un encabezamiento que contiene:
  - Direcciones fuente y destino
  - Tipo de datagrama
- El protocolo IP intenta entregar paquetes pero no garantiza la entrega
- Los paquetes pueden perderse, duplicarse y llegar en distinto orden

Tiempo de vida de datagrama

- Datagramas pueden circular indefinidamente
  - Consume recursos de enlaces y nodos
  - Protocolo de Transporte pone límites
- Datagramas marcados con tiempo de vida
  - Campo especial en IP (*Time To Live*)
  - Una vez que expira, se descarta
  - Cuenta de saltos: decrementa tiempo de vida cada vez que pasa por un router
  - Cuenta de tiempo: cuánto hace que pasó por un router

Fragmentación y re-armado

- Causado por los diferentes tamaños de paquetes soportados por las redes que se atraviesa
- Rearmado se puede hacer:
  - En el destino
    - Resulta paquetes más chicos al cruzar la red
  - En nodos intermedios
    - Necesita buffers grandes en routers
    - Buffers pueden llenarse con fragmentos
    - Todos los fragmentos van hacia el mismo router

Parámetros

- MSS (*Maximun Segment Size*) es la longitud de un segmento de datos que una capa entrega a la inferior
- Ejemplos:
  - Datagrama IP puede tener 65535 octetos
  - Trama Ethernet puede tener 1500 octetos
- MTU (*Maximun Transmission Unit*) es el límite del campo de datos que puede transportar un protocolo

Criterios

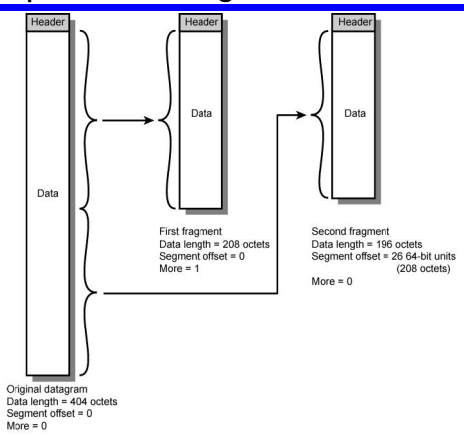
- Si el MSS es mayor que el MTU hay fragmentación: los routers dividen un datagrama entre varias tramas
- Los fragmentos a su vez pueden ser fragmentados nuevamente si pasan por una red de menor MTU
- En el extremo de llegada se rearman los fragmentos que llegan dentro de un tiempo establecido (si no se descarta)

Fragmentación IP

- IP rearma sólo en destino
- Usa campo en encabezamiento
  - *Data Unit Identifier* (ID)
    - Identifica si el sistema es terminal
      - Dirección fuente y destino
      - Capa que genera datos
      - Identificación entregada por esa capa
  - Longitud de datos
    - Datos de usuario expresado en octetos

  - Desplazamiento (*Offset*)
    - Indica la posición del fragmento de datos de usuario en el datagrama original
    - Se expresa en múltiplos de 64 bits (8 octetos)
  - Bandera (*More*)
    - Indica que éste no es el último fragmento

Ejemplo de Fragmentación



Tratamiento de fallas

- Rearmado puede fallar si se pierden fragmentos
- Hay necesidad de detectar fallas
- Tiempo para rearmado
  - Asignado al primer fragmento que llega
  - Si expira antes de que lleguen todos, descarta datos
- Usar tiempo de vida de paquetes (*time to live*)

Control de errores

- IP no garantiza la entrega del mensaje
- Router debería informar a la fuente que descartó paquetes
- La fuente puede modificar la estrategia
- Puede informar a capas superiores
- Necesita identificar datagramas
- Ver ICMP más adelante

Control de flujo

- Permite a routers y/o estaciones limitar la velocidad de entrada de datos
- Limitado a sistemas sin conexión
- Envía paquetes de control de flujo pidiendo reducirlo

Internet Protocol (IP) Versión 4

- Parte del conjunto TCP/IP
- Especifica interfaz con capas superiores (TCP)
- Especifica formatos y mecanismos
- Descripto en RFC 791
- Se lo reemplazará por IPv6

Servicios IP

- Primitivas
  - Funciones a realizar
  - Forma depende de implementación
  - Ejemplos:
    - **Send** (pide la transmisión de una unidad de datos)
    - **Deliver** (notifica al usuario que llegó una unidad de datos)
- Parámetros
  - Usados para pasar datos e información de control

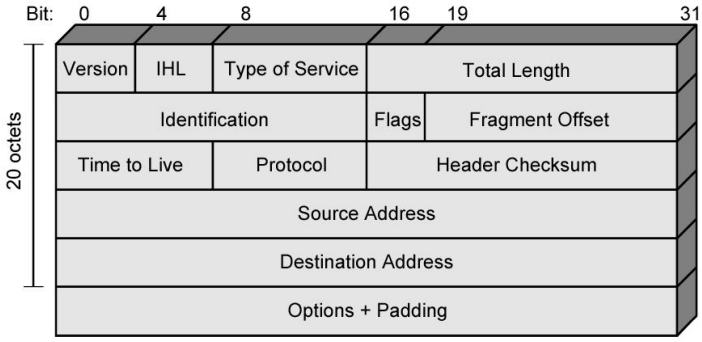
Parámetros fijos

- Dirección fuente
- Dirección destino
- Protocolo
- Tipo de Servicio
- Identificación
- Indicador de “no fragmentar”
- Tiempo de vida
- Longitud de datos
- Datos opcionales
- Datos de usuario

Parámetros opcionales

- Seguridad
- Ruteo fuente
- Registro de ruta
- Identificación de la secuencia
- Estampa de tiempo

Encabezamiento IPv4



Campos del encabezamiento

- Versión del protocolo: 4 ó 6
- Longitud del encabezamiento (IHL)
  - Expresado en palabras de 32 bit
  - Incluye opcionales
  - Generalmente vale 5
- Tipo de servicio:
  - Bits 0 a 2 definen prioridades del tráfico
  - Bit 3 bajo retardo
  - Bit 4 alta velocidad
  - Bit 5 alta confiabilidad
  - Bits 6 y 7 están reservados
- Longitud total del datagrama: se expresa en octetos

- Identificación: usado para armar paquetes fragmentados
- Flags
  - Bit 0 reservado
  - Bit 1: pide no fragmentar
  - Bit 2: indica el último paquete fragmentado
- Desplazamiento de fragmentación:
  - Sirve para armar paquetes fragmentados
  - El primero es cero
- Tiempo de vida
- Protocolo: definido en las RFC 790 y 1010
  - Ejemplo: para TCP es 06h, para UDP es 11h

- *Checksum* del encabezamiento
  - Reverificado en cada router
  - Es el complemento a 1 de la suma de todas las palabras de 16 bit del encabezamiento
- Dirección fuente
- Dirección destino
- Opcionales:
  - Puede haber hasta 40 bytes
  - El primero tiene un flag de copy, dos bits de clase de opciones y cinco bits de número de opción
- Relleno: para tener longitud múltiplo de 32 bits

Campo de datos

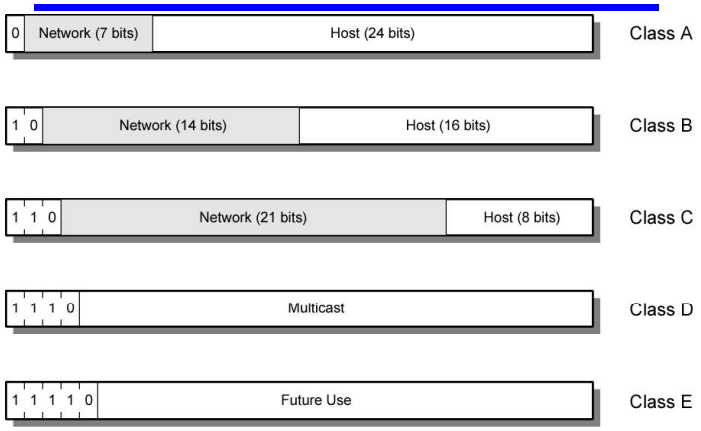
- Pasa datos a la siguiente capa
- Múltiplo entero de 8 bits
- Máxima longitud del datagrama (encabezamiento y datos): 65.535 octetos

Direccionamiento v4

- La dirección de un equipo en la red permite identificarlo y rutear el tráfico hacia el mismo
- Es un binario de 32 bits divididos en cuatro octetos con representación decimal separados por puntos (10.4.60.0)
- Tiene dos partes:
  - —Prefijo: la dirección de la red (network)
  - —Sufijo: la dirección del equipo (host)
- El campo de host no identifica una computadora sino la interfaz de conexión a la red
- Hay varias clases, repartiendo los octetos entre network y host

- Valores especiales
  - — Dirección de red: bits de host en 0
  - — Dirección de broadcast local: bits de network y host en 1
  - — Dirección de broadcast remoto: bits de host en 1
- Las direcciones son asignadas por:
  - — Prefijos: una autoridad central o el proveedor de servicios
  - — Sufijos: el administrador local
- Los *host multi homed* tienes dos interfaces y dos direcciones para aumentar confiabilidad

Formatos de direccionamiento IPv4



Direcciones IP - Clase A

- Comienzan con binario 0
- La dirección “Todos 0” está reservada
- Rango: desde 1.x.x.x hasta 126.x.x.x
- Permite 126 redes, cada una con 16.777.214 computadoras

Direcciones IP - Clase B

- Comienzan con binario 10
- Rango: de 128.x.x.x hasta 191.x.x.x
- Segundo Octeto también incluido en dirección de la red
- Permite 16.384 redes, cada una con 65.534 computadoras

Direcciones IP - Clase C

- Comienzan con binario 110
- Rango: de 192.x.x.x hasta 223.x.x.x
- Segundo y tercer octeto también son parte de dirección de la red
- Permite 2.097.152 redes de 254 computadoras

Direcciones reservadas

- Las direcciones reservadas y las privadas no deben aparecer en Internet
- Las reservadas por distintas RFC son:
  - 100.64.0.0/10: direcciones compartidas
  - 127.0.0.0 /127.255.255.255: para hacer loopback (no pasa a capas inferiores)
  - 169.254.0.0./16: enlace local
  - 192.0.0.0/24 y 192.0.2.0/24
  - 192.88.99.0/24: enlace entre v4 y v6
  - 198.18.0.0/15, 198.51.100.0/24 y 203.0.113.0/24
  - 224.0.0.0/239.255.255.255: clase D (para multicast)
  - 240.0.0.0/255.255.255.255: clase E
- Las direcciones privadas se ven más adelante

Proxy ARP

- Las clase de direcciones IP son rígidas y desperdician bits que se pueden necesitar en el otro campo
- Hay dos mecanismos para flexibilizar: Proxy y Subredes
- Un router con proxy ARP:
  - Hace que todas las máquinas de dos redes trabajen como conectadas a una sola red
  - No hay cambios a la tabla del router
  - Trabaja sólo en redes con ARP
  - Generalmente se configura manualmente

Subredes

- No estaban previstas en el protocolo original
- Permite utilizar el mismo prefijo para varias redes
- Divide el campo de host en subred y host
- Para dimensionar cada campo se debe analizar la cantidad de redes y de computadoras a conectar
- La técnica de “subnetting” proporciona una cantidad de subredes mientras que reduce el número de Host de cada subred.
- Para analizar las direcciones se asignan máscaras de 32 bits con 1 en prefijo y 0 en sufijo

Máscaras Naturales

Clase A	255. 0. 0. 0.
Clase B	255. 255. 0. 0.
Clase C	255. 255. 255. 0.

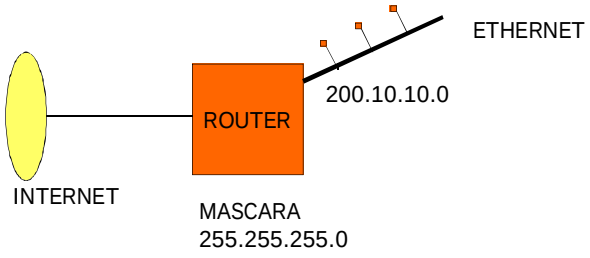
- La máscara permite separar bits del campo de host para numerar subredes
- Ejemplo: máscara para la direccion clase C

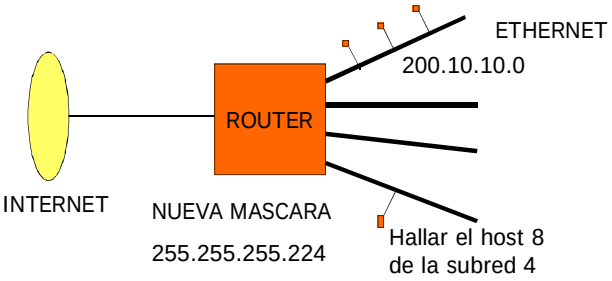
194 . 8 . 8 . 72
11000010 . 00001000 . 00001000 . 01001000

Máscara sin subredes 11111111 . 11111111 . 11111111 . 00000000
Host número 72 de la red 194.8.8.0

Máscara con subredes 11111111 . 11111111 . 11111111 . 11100000
01001000
Host número 8 de la subred 2 de la red 194.8.8.0
Máscara 255.255.255.224

Generación de subredes





DIRECCION DEL HOST NUMERO 8 DE LA SUBRED 4

200.10.10.10001000

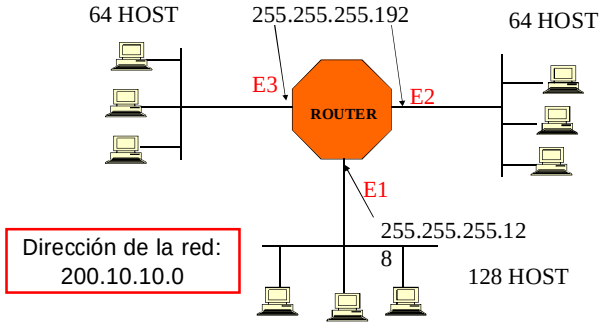
200.10.10.136

Subredes potenciales de clase C (No incluye numero de red y difusión)

Mascara (Decimal)	Mascara (Binario)	Numero de Subredes	Numero de Host
128	1 0 0 0 0 0 0 0	2	128
192	1 1 0 0 0 0 0 0	4	64
224	1 1 1 0 0 0 0 0	8	32
240	1 1 1 1 0 0 0 0	16	16
248	1 1 1 1 1 0 0 0	32	8
252	1 1 1 1 1 1 0 0	64	4

Problema

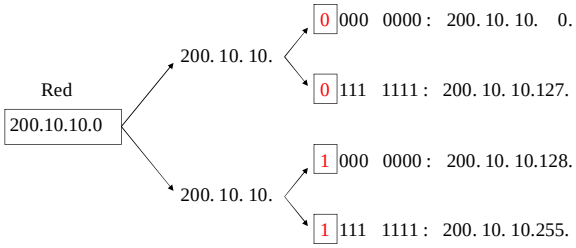
Dada una dirección clase C: 200.10.10.0, asignar las direcciones a las siguientes redes:



Ejemplo de VLSM

Primer máscara: 255.255.255.128

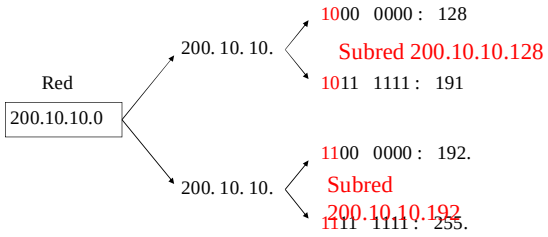
Se obtienen 2 subredes 128 host c/u



Rango de direcciones: 200.10.10.0 - 200.10.10.127

Segunda máscara: 255.255.255.192

Se obtienen 2 subredes 64 host c/u



Rango de direcciones: 200.10.10.128 - 200.10.10.255

Configuración de las interfaces

- INTERFAZ E1 (128 HOST)
  - —NUMERO DE RED: 200.10.10.0
  - —MASCARA: 255.255.255.128
  - —RANGO DIRECCIONES
  - —200.10.10.0 A 200.10.10.127

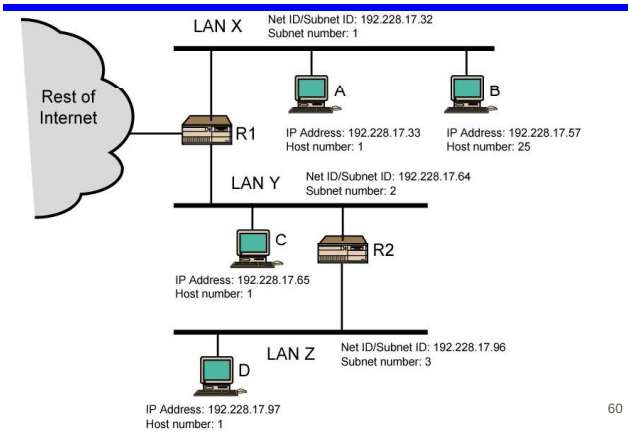
- INTERFAZ E2 (64 HOST)
  - —NUMERO DE RED: 200.10.10.128
  - —MASCARA: 255.255.255.192
  - —RANGO DIRECCIONES
  - —200.10.10.128 A 200.10.10.191

- INTERFAZ E3 (64 HOST)
  - —NUMERO DE RED: 200.10.10.192
  - —MASCARA: 255.255.255.192
  - —RANGO DIRECCIONES
  - —200.10.10.192 A 200.10.10.255

Máscaras

- Hay dos tipos de máscaras: de longitud fijas y variable
- Las máscaras de longitud fija son iguales en toda la red y en algunos puntos genera desperdicio de bits
- VLSM (*Variable lenght Subnet Mask*): en cada red la longitud de la máscara es asignada por el administrador
- Es más complejo pero optimiza el direccionamiento
- Si bien se puede, no conviene:
  - — Asignar subredes con todos 0 o todos 1
  - — Asignar bits en redes no contiguas
- En los routers con protocolos que lo soportan, para cada dirección hay una máscara

Ruteo usando subredes



CIDR

- CIDR (*Claseless Inter Domain Routing*) permite extender la asignación de direcciones en Internet hasta que se amplíe el direccionamiento con la versión 6
- Es compatible con el esquema anterior (*Clasefull*)
- Extiende el uso de VLSM a los prefijos
- Permite agregar bits a una dirección clase C y direccionar más redes
- Las direcciones se indican como: Prefijo/Long.de máscara
- La longitud de la máscara debe convertirse a 32 bits en cada router

- ENTRE 1991 Y 1995 SE DUPLICARON LAS TABLAS DE ENRUTAMIENTO DE LOS ROUTERS CADA 10 MESES.
- CON ESTA PROYECCION EN 1995 HUBIERAN LLEGADO A 80.000 RUTAS SIN EMBARGO EN EL 2001 NO SUPERAN LAS 76.000.
- LA REDUCCION SE LOGRO EN BASE A LA ADOPCION DE CIDR.
- 200.10.0.0 MASCARA 255.255.0.0 SE CONVIERTE EN 200.10.0.0 /16 (PREFIJO)

Direccionamiento CIDR

Dirección clase C: 198.32.1.0

Máscara: 255.255.255.0 (NATURAL)

11111111 11111111 11111111 00000000

11000110 00100000 00000001 00000000

198.32.0.0 / 16 EQUIVALE A MASCARA 255.255.0.0

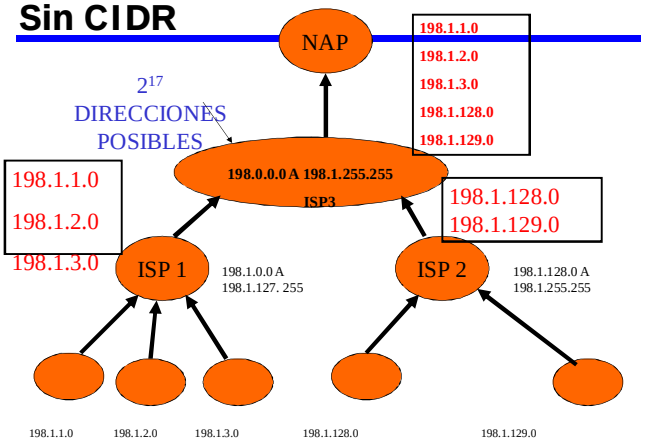
11111111 11111111 00000000 00000000

Se habla de SUPER RED cuando la máscara es inferior a la natural

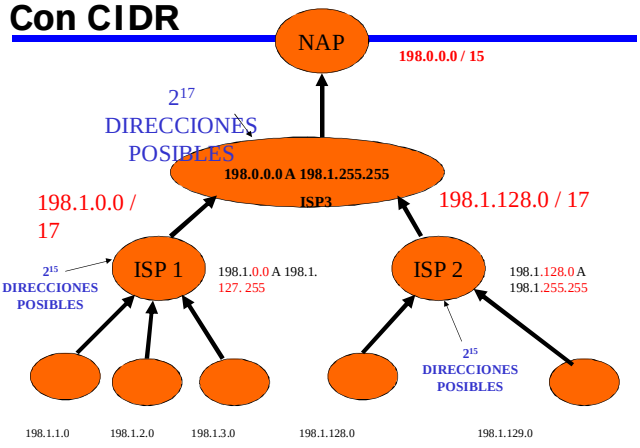
Ventajas de CIDR

- LOS DOMINIOS QUE SOPORTAN CIDR SE DENOMINAN SIN CLASE.
- CIDR GENERA UNA ARQUITECTURA MAS JERARQUICA, CADA DOMINIO TOMA SU DIRECCION DEL NIVEL SUPERIOR.
- ESTO GENERA UN AHORRO EN LA PROPAGACION DE LA RUTA.
- EL ISP PUBLICA UNA UNICA RUTA EN LUGAR DE MUCHAS INDIVIDUALES. (AGREGACION DE RUTAS), DIMINUYENDO LAS TABLAS DE ENRUTAMIENTO.

Sin CIDR



Con CIDR



Asignación por bloques

Restricciones a la asignación de direcciones sin clase:
- Las direcciones del bloque deben ser consecutivas.
- El número de direcciones del bloque debe ser potencia de 2.

40.6.7.32
40.6.7.33
40.6.7.34
……
40.6.7.47

16 direcciones consecutivas

La forma x.y.z.t / n define el bloque
En el ejemplo anterior: 40.6.7.32 / 28

00101000. 00000110. 00000111. 00100000
Primera dirección del bloque
40 6 7 32

00101000. 00000110. 00000111. 00101111
Ultima dirección del bloque
40 6 7 47

Cantidad de direcciones = $2^n = 2^4 = 16$

Otro método

Mediante la máscara, dada una dirección del bloque
- Primera dirección mediante una AND con la máscara y la direccion dada.

- Ultima dirección mediante una OR al complemento de la máscara

El número de direcciones sale mediante el complemento a uno de la máscara sumando uno.

Ejemplo

Hallar la primera y última dirección del bloque, del cual una dirección dada es la siguiente, e indicar el número de direcciones del mismo:

32.4.3.16 / 26

00100000. 00000100. 00000011. 00010000.
111111111. 111111111. 111111111. 11000000 (Máscara)
AND
00100000. 00000100. 00000011. 00000000 (Dirección más baja)
32 4 3 0
OR
00000000. 00000000. 0000000. 00111111 (Complemento de la máscara)
00110000. 00000100. 00000011.00100000
32 4 3 63 (. 00111111)

Número de direcciones:
0000000. 00000000. 00000000. 00111111 = 63 + 1 = 64 direcciones

Dirección de Red

La primera dirección del bloque es la dirección de red.

PREFIJO + SUBFIJO

PREFIJO ES LA RED, EL SUBFIJO ES EL HOST.

40.3.2.33 / 26

00101000. 00000011. 00000010. 00100001
Los 26 bits a la izquierda definen la red : 40.3.2.0

Los 32 – 26 bits a la derecha definen el host: host 33

Subredes

• Se tiene la red 10.2.4.0/26 y se desea tener tres subredes de: 32 dir. subred 1, 16 dir. subred 2 y 16 dir. subred 3 cada una.

• SOLUCION:
Tomar una máscara /27, el ultimo octeto quedará:
00000000 a 00011111. Subred 1 (host 0 a 31)

Para las otras dos subredes el tercer bit es uno y se debe tomar una máscara /28, el ultimo octeto quedará:
00100000 a 00101111 Subred 2 (host 32 a 47)
00110000 a 00111111 Subred 3 (host 48 a 63)

Direcciones privadas

- Son bloques CIDR para uso local de una organización
- Sirven a un grupo cerrado de host y son seguras
- Nunca debe aparecer en Internet
- Son las siguientes:

Prefijo	Desde	Hasta
10/8	10.0.0.0	10.255.255.255
172.16/12	172.16.0.0	172.31.255.255
192.168/16	192.168.0.0	192.168.255.255
169.254/16	169.254.0.0	169.254.255.255

NAT

- *Network Address Translation*: protocolo manejado por un router en la frontera entre una red con direcciones privadas y la Internet
- Protocolo descripto en RFC 1631
- Al pasar por el router se modifican las direcciones en el encabezamiento
- NAT debe conocer los ports de transporte para enrutar destinos NAPT (*Network Address and Port Translation*)
- NAT tiene problemas con muchas aplicaciones porque debe cambiar:
  - Direcciones IP
  - Ports
  - Checksum de encabezamientos
  - Mensajes ICMP

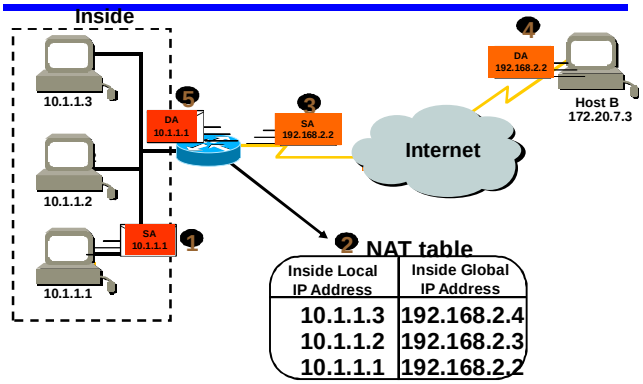
- Ventajas:
  - Todas las máquinas de la red privada comparten el uso de algunas direcciones públicas para acceder a servidores en Internet
  - Facilita la administración y la seguridad
- Desventajas
  - Algunas aplicaciones necesitan trabajar con direcciones públicas
  - Reduce performance
  - Permite poco soporte para los clientes

- NAT convierte direcciones privadas en públicas mediante programas:
  - slirp (Unix)
  - masquerade (Linux)
  - Internet Connection Sharing (Microsoft)

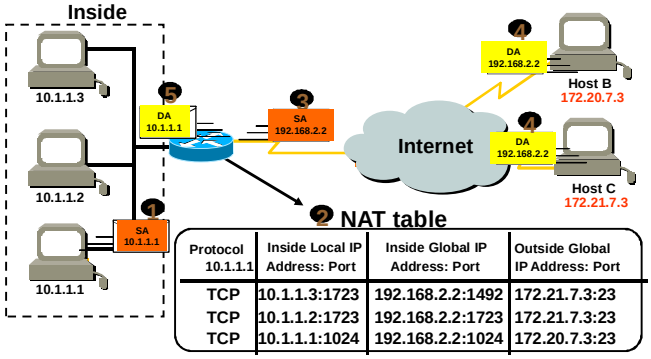
NAT

- Estático.
- Dinámico.
- PAT: *Port Address Translation* (Traducción de Direcciones por Puerto)
- Sobrecarga.

Conversión de direcciones internas



Overloading Inside Global Addresses



VPN

- VPN (*Virtual Private Network*) permite pasar datos entre redes privadas a través de la red pública haciendo encriptación o túnel IP
- En cada acceso a la red privada hay sólo una dirección pública compartida y se usa NAT
- La red privada se conecta al POP del ISP mediante un enlace PPP que utiliza:
  - NAS o LAC: concentrador de acceso
  - LNS: servidor de red

- El túnel es una conexión protegida con ancho de banda garantizado entre NAS y LNS
- Opera en capa 2 y utiliza alguno de los protocolos específicos:
  - PPTP: *Point To Point Tunneling Protocol*
  - L2TP (*Layer 2 Tunneling Protocol*): desarrollado por el IETF combinando y mejorando las facilidades de los protocolos anteriores

ACL: Listas de control de acceso

Se configuran en los routers con el formato:

access-list # permit/deny source IP wildcard

donde:

= 1-99 (Standards), Numero de ACL

permit/deny: encaminar el paquete o descartarlo

source IP - Direccion IP de origen contra la cual se comparara el paquete , puede ser tambien ANY.

wildcard (Mascara Inversa)

Wildcard: máscara inversa

Permite especificar un host, una subred, una red o un rango de direcciones IP.

Los dos valores binarios (0 y 1) tienen diferentes valores en una wildcard :

0 = Debe coincidir exactamente

1 = Ignorar

Ejemplos de ACL

- Ejemplo 1:

A(config)#access-list 5 deny 172.22.5.2 0.0.0.0
A(config)#access-list 5 deny 172.22.5.3 0.0.0.0
A(config)#access-list 5 permit any

Si un paquete desde 172.22.5.2 llega a este router el mismo será descartado (DROP)

Si proviene de la IP 172.22.5.3, también

Permite que pase todo el resto del tráfico IP

Ejemplos de wild cards

IP Origen	Wildcard
195.34.5.12	0.0.0.0

Solicitud : Match los 4 octetos
Solo 195.34.5.12 es coincidencia

Se podria utilizar la sintaxis Host 195.34.5.12 en lugar de la Wildcard, ya que Host indica un match exacto y único

IP Origen	Wildcard
172.16.10.0	0.0.0.255

Resultado: Que concuerden los 3 primeros octetos y el 4to. No importa

Los valores "0" en la wildcard significan que los bits de la IP deben concordar exactamente con la propuesta.

Los Valores "1" son ignorados en la wildcard. (255 = todos 1's binarios.)

172.16.10.0 hasta 172.16.10.255 es una concordancia con el criterio de selección, entonces cualquier valor de IP entre 172.16.10.0 y 172.16.10.255 será permitido pasar a través de la ACL.

IP Origen	Wildcard
172.16.10.0	0.0.31.255

Concentrese en el tercer octeto :

31 en binario es 00011111
debe coincidir — no importa
10 en binario es 00001010

Los primeros 3 bits deben ser 0's y los ultimos 5 bits no importan.

Los valores aceptables en la ACL van desde 172.16.0.0 hasta 172.16.31.255

Los valores aceptables van desde 172.16.0.0 hasta 172.16.31.255

Un valor de 172.16.32.0 no coincidiria con el criterio dado que 32 en binario = 00100000 y esto no es igual a los 3 bits que se comparaban para matchear.

31 en binario es 00011111
debe coincidir — No importa
10 en binario es 00001010

IP Origen	Wildcard
172.16.64.0	0.0.31.255

Concentrese en el tercer octeto

31 en binario es 00011111
deben coincidir — No importa
64 en binario es 01000000

Entonces los 3 primeros bits deben ser 010 y los utimos 5 bits no importan.

Que rango de IP's seran aceptables para esta wildcard?

IP Origen	Wildcard
172.16.64.0	0.0.31.255

Concentrece en el tercer octeto

31 en binario es 00011111

debe coincidir — no importa

64 en binario es 01000000

Los valores aceptables son 01000000 = 64 hasta 01011111 = 95

IP Origen	Wildcard
10.0.0.0	0.0.255.255

Los dos primeros octetos deben coincidir, asi que todas las direcciones IP que empiecen con 10.0 son coincidencias

El rango de direcciones IP permitidas o denegadas sera desde 10.0.0.0 hasta 10.0.255.255

Protocolo ARP

- Convierte direcciones de red (IP) en direcciones de hardware (MAC)
- Las aplicaciones sólo manejan direcciones de red
- Dos tipos de mapeo:
  - Directo (redes pequeñas): algunos bits de la dirección IP contienen la dirección MAC
  - Dinámico (redes grandes)
- ARP: (*Address Resolution Protocol)* dentro de una LAN
  - manda un mensaje de broadcast llamando a una computadora por su dirección de red
  - cuando el identificado contesta, se puede ver su dirección de hardware en la trama

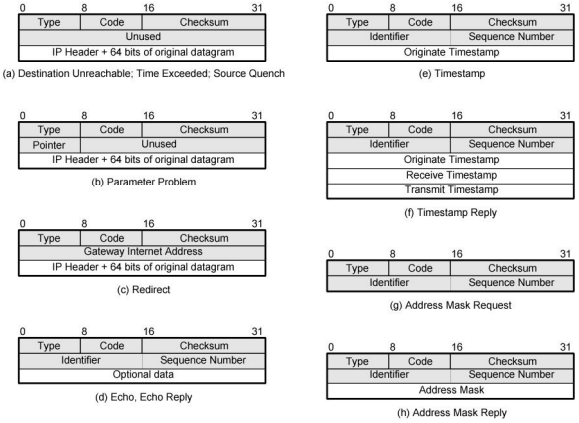
- Correspondencia entre direcciones IP y MAC se guarda en una tabla que se refresca cada 20 min
- Mensajes ARP se encapsulan sobre Ethernet
  - Se rellenan con ceros para dar longitud mínima
  - Tipo de datos: 0x0806
- RARP (Reverse Address Resolution Protocol)
  - A partir de la dirección MAC consulta por la IP
  - Usa el mismo formato de paquetes que ARP

ICMP versión 4

- ICMP *(Internet Control Message Protocol)*: utilizado por los router para informar al origen los problemas detectados a su nivel
- Descripto en la RFC 792
- Transferencia de mensajes de control de routers y computadoras a las computadoras
- Es una realimentación ante la existencia de problemas
- No son mensajes confiables porque van encapsulados en datagramas IP

- El checksum del encabezamiento IP detecta errores de trasmisión
- Los mensajes ICMP van encapsulados en datagramas IP, ocupando el campo de datos
- Hay varios formatos de mensajes
- Son funciones ICMP
  - Ping (prueba de enlace)
  - Redireccionar
  - Tiempo excedido (se descartó datagrama por tiempo de vida)

Formatos de Mensajes ICMP



IP v6

Versiones del protocolo IP

- IP v 1-3: definidos y reemplazados
- IP v4 : versión actual
- IP v5 : versión intermedia sin implementar
- IP v6 : nueva versión
  - — reemplaza a IP v4 desde 2008 a 2011 para toda la red del gobierno de USA
  - — durante el desarrollo se lo llamó IPng (nueva generación)

Razones para el cambio

- Se agotan las direcciones IP:
  - — El direccionamiento de dos niveles (red y computadora) desperdicia espacio
  - — La dirección de red se usa aún si no se conecta a Internet
  - — El crecimiento de las redes y de Internet
  - — El uso extendido de TCP/IP
- Hay una sola dirección por computadora
- Hay nuevos tipos de servicios que no se pueden cursar

Las RFC para IPv6

- 1752: Recommendations for the IP Next Generation Protocol
- 2460: Overall specification
- 2373: Addressing structure

Mejoras de IPv6

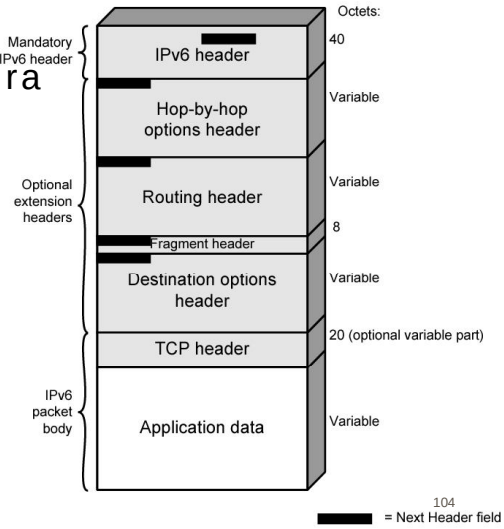
- Mayor espacio para direccionar: 128 bit
- Opcionales mejorados
  - — Separa encabezamiento de optionales en dos partes
    - capa IP
    - capa Transporte
  - — La mayoría no son examinados por routers intermedios
    - Mejora velocidad y simplifica procesamiento de routers
    - Facilidad para ampliaciones
- Direcciones autoconfigurables
  - — Asignación dinámica

- Direccionamiento más flexible
  - — Permite mandar mensajes a una serie de nodos (*Anycast*)
  - — Mejora la ampliación de direcciones múltiples (*Multicast*)
- Permite asignación de recursos
  - — Reemplaza a tipos de servicio
  - — Rotula paquetes para un flujo de tráfico especial
    Ejemplo: video en tiempo real

Procesamiento simplificado

- El encabezado es más simple.
- Los campos poco utilizados son ahora OPCIONES.
- No se realiza fragmentación.
- No hay *checksum* (se deja para el TCP o UDP)
- El campo TTL (*time to live*) pasa a llamarse **Limite de Saltos**

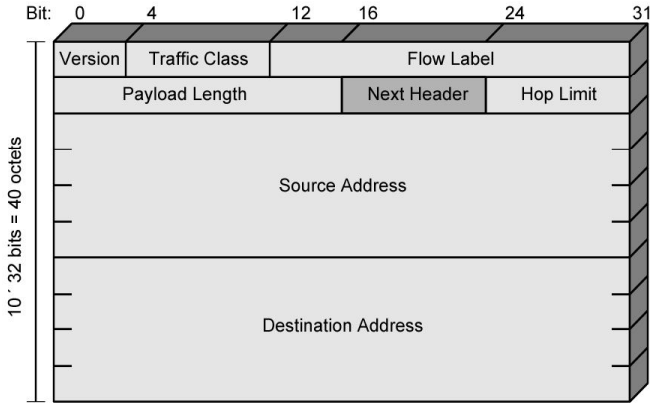
IPv6: Estructura



Opcionales del encabezamiento

- Opciones salto a salto
  - Requiere procesamiento en cada router
- Ruteo
  - Similar al ruteo de v4
- Fragmentación
- Autenticación
- Encapsula información de seguridad
- Opcionales para nodo destino

Encabezamiento de IPv6



Campos del encabezamiento

- Version
  - 6
- Clase de Tráfico
  - Prioridades de paquetes
  - Aún en desarrollo
  - Ver RFC 2460
- Rótulo de flujo
  - Usado por computadoras que piden tratamiento especial
- Longitud de datos (*payload*)
  - Incluye encabezamientos de capas superiores y datos del usuario

- Próximo encabezamiento
  - Identifica tipo de encabezamiento
  - Extensión de capa superior
- Dirección fuente
- Dirección destino

Etiquetas de Flujo

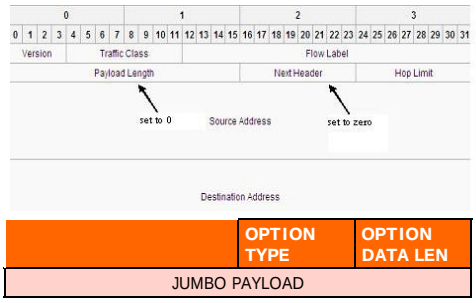
- Este campo de 20 bits puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6:
  - -calidad de servicio no estándar
  - - servicio en "tiempo real".
- Todavía es experimental y sujeto a cambios
- Se exige a los hosts o a los enrutadores que no dan soporte a las funciones del campo Etiqueta de Flujo:
  - poner el campo a cero al originar un paquete
  - pasar el campo inalterado al reenviar un paquete
  - ignorar el campo al recibir un paquete.

Clases de Tráfico

- El campo de 8 bits Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6.
- Hay varios experimentos en curso para el uso de los bits Tipo de Servicio IPv4 destinados a proporcionar varias formas de "servicio diferenciado" para paquetes IP.

Longitud de la carga util

- IPv6 requiere un MTU minimo de 1280 bytes.
- Si el enlace es más chico, la fragmentacion y reensamblado debe ser provista por una capa inferior.
- Se recomienda que los nodos IPv6 implementen un metodo para descubrir el MTU mínimo (RFC 1981).
- Se admite la existencia de JUMBOGRAMAS.
- El maximo normal es de 64 kbytes pero se puede extender mediante la *JUMBO PAYLOAD OPTION* a 4 Gbytes
- No implementado (por ahora es sólo para redes privadas)



	OPTION TYPE	OPTION DATA LEN
JUMBO PAYLOAD		

Cabecera de Extensión

LOS ENCABEZADOS DE DATOS Y ESTADO NO LLEVAN EXTENSIONES

Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete.

RFC 2460 Ruteo (*Routing*) Métodos para especificar la forma de rutear un datagrama. (Usado con IPv6 móvil)RFC 2460, RFC 6275,
RFC 5095 Cabecera de fragmentación (*Fragment*) Contiene parámetros para la fragmentación de los datagramas.
RFC 2460 Cabecera de autenticación (*Authentication Header (AH)*) Contiene información para verificar la autenticación de la mayor parte de los datos del paquete.
RFC 4302Encapsulado de seguridad de la carga útil (*Encapsulating Security Payload (ESP)*)50variableLleva la información cifrada para comunicación segura.
RFC 4303 Opciones para el destino (*Destination Options*) Información que necesita ser examinada solamente por los nodos de destino del paquete.
RFC 2460 *No Next Header* Indica que no hay más cabeceras

Cabeceras de extension

TIPO	SIGNIFICADO
0	Hop by hop Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete
43	Encabezado de enrutamiento
44	Encabezado de fragmentación Contiene parámetros para la fragmentación de los datagramas
50	Encapsulado de seguridad de la carga útil Lleva la información cifrada para comunicación segura
51	Cabecera de autenticación Contiene información para verificar la autenticación de la mayor parte de los datos del paquete
59	NO Next Header. No hay mas cabeceras de extension
60	Encabezado de opciones de destino

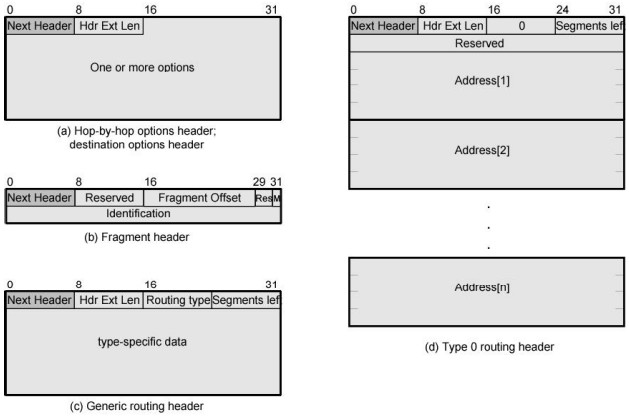
Encabezados sin Next Header

TIPO	SIGNIFICADO
6	TCP
17	UDP
58	ICMPv6
59	"NO HAY PROXIMA CABECERA"

Ejemplo

IPv6 HEADER	Routing Header	TCP Header y Datos
Next Header: 43	Next Header: 6	

Encabezamiento extendido



Limite de saltos

- Reemplaza el campo *"TTL"* (*Time-to-Live o Tiempo de vida*) en IPv4.
  - -Su valor (de 8 bits) disminuye con cada nodo que reenvía el paquete.
  - -Si este valor llega a 0 cuando el paquete IPv6 pasa por un router, se rechazará y se enviará un mensaje de error ICMPv6.
  - - Esto se utiliza para evitar que los datagramas circulen indefinidamente.
- Tiene la misma función que el campo *Time to live,* representa la cantidad de saltos y disminuye con cada paso por un router.
- Como nadie usa el tiempo en segundos, se ha cambiado el nombre para que refleje su verdadero uso.

Direcciones de IPv6

- Asignadas a la interfaz, no a la computadora
- Una sola interfaz puede tener varias direcciones
- Largo de 128 bits
- Dividida en 8 grupos de 4 dígitos hexadecimales separados por dos puntos:
  - Ejemplo 4fa6:3d65:4999:af43:b67a:0dfa:0000:abcd
- Si aparecen cuatro puntos indica que se ha comprimido un grupo de cuatro ceros

ARQUITECTURA DE DIRECCIONES

PREFIJO	USO
::0/96	SIN ESPECIFICAR. COMPATIBLE CON DIRECCIONES IPv4
::FFFF:0.0.0.0/96	DIRECCIONES IPv4
200::/7	RESERVA PARA LOCACIONES NSAP
400::/7	RESERVADA PARA LOCACIONES ISP
2000::/3	UNICAST GLOBAL (RFC 3587)
FE80::/10	UNICAST LINK LOCAL
FEC0::/10	UNICAST SITIO LOCAL (RFC 3879)
FC00::/7	Propuesta de UNICAST LOCAL IPv6
FF00::/8	MULTICAST

Direcciones de IPv4 y v6

- Una dirección v6 puede tener los últimos 32 bits con una dirección v4
- IPv4 mapeada: ::FFFF:192.168.89.9
- IPv4 compatible: ::192.168.89.9
- TEREDO: es un mecanismo de transición entre las versiones 4 y 6
  - Embebido en Windows Vista
  - Clientes en red 4 privada con NAT manejan tablas de equivalencia entre versiones
  - Servidores interconectan redes 4 y 6
  - Paquetes IP6 se encapsulan en mensajes IP4/UDP

Tipos de direciones v6

- *Unicast*
  - Interfaz única, similar a dirección pública de v4
- *Anycast*
  - Serie de interfaces (diferentes nodos)
  - Mensajes entregados al nodo más cercano
- *Multicast*
  - Serie de interfaces
  - Mensajes entregados a todos los nodos

Direcciones unicast y anycast

Bits	48 (o mas)	16 (o menos)	64
campo	Prefijo de ruteo	Subnet id.	Identificador de interface

- El **prefijo de ruteo** *(routing prefix)* o prefijo de encaminamiento junto con el identificador de subred *(subnet id)*) está situado en los 64 bits más significativos de la dirección ipv6. El tamaño del *routing prefix* puede variar; un prefijo de mayor tamaño significa un tamaño menor para *subnet id*.
- El ***subnet id*** permite a los administradores de red definir subredes dentro de la red disponible.
- Los 64 bits de **identificador del interface** *(interface identifier)* son generados automáticamente con la dirección MAC del interface y el algoritmo EUI-64 modificado, obtenidos de un servidor DHCPv6, establecidos aleatoriamente o asignados manualmente.

Unicast local

Son similares a las direcciones IPv4 publicas

2001::/16	REGISTROS REGIONALES DE INTERNET	RFC 2450
2002::/16	MECANISMOS DE RETRANSMISION 6 to 4	RFC 3056
3FFE::/16	RED 6 BONE TEXT	RFC 2471 RFC 3701

RIR: Regional Internet Register

El RIR es responsable de entregar bloques menores a los LIR (Local Internet Registers), quienes generalmente son ISP (Internet Service Provider), quienes a su vez los asignan al usuario final.

ES LA FORMA NORMAL DE DIRECCIONAR

Direcciones de enlace local

Bits	10	54	64
campo	Prefijo de ruteo Fe80::/10 1111111010	Todos ceros	Identificador de interfase

- SON NO RUTEABLES
- Son direcciones con significado solo en enlaces locales.
- *Link: es un grupo de maquinas que se pueden comunicar directamente sin la intervención de un Router IPv6*
- Pueden ser
  - -Punto a Punto
  - -Broadcast
  - -Cualquier cosa
- **SON EL EQUIVALENTE A DIRECCIONES PRIVADAS**

Algoritmo EUI-64.

Genera direcciones de una interface MAC a IPv6

EJ: **MAC 00:50:8b:c8:e6:76**

Se coloca un 1 en el 7mo bit (el que identifica local/universal) con lo que el 1er byte queda:

00 queda 02 : 0000 0010

Queda 02:50:8b:c8:e6:76

Lo divide en dos partes de 8 bytes c/una 02:50:8b y c8:e6:76 y le inserta entre ellas el valor ff:fe

02:50:8b:ff:fe:c8:e6:76

Direccion multicast

Bits	8	4	4	112
Campo	prefijo	flags	Scope (ambito)	ID de grupo
valor	11111111	0RPT	XXXX	

FLAGS

Flag	0	1
R (Rendevous)	**No** tiene codificado en la direccion el nodo que da la solucion de ruteo	**SI** tiene codificado en la direccion el nodo que da la solucion de ruteo
P (Prefijo)	Sin información de prefijo	Dirección basada en prefijo de red
T (Transitoria)	Multicast mundialmente valida (permanente)	Asignada dinámicamente (temporal)

Scope

Es el ámbito (scope) que indica en que partes de la red es valida la dirección

Valor	significado
0x0	Reservado
0x1	Nodo local
0x2	Link Local
0x5	Sitio Local
0x8	Organización Local
0xe	global
0xf	reservado
Resto de los valores sin asignar	

Direcciones IPv6

PREFIJO	USO
::0/96	SIN ESPECIFICAR. COMPATIBLE CON DIRECCIONES IPv4
::FFFF:0.0.0.0/96	DIRECCIONES IPv4
200::/7	RESERVA PARA LOCACIONES NSAP
400::/7	RESERVADA PARA LOCACIONES IPS
2000::/3	UNICAST GLOBAL (RFC 3587)
FE80::/10	UNICAST LINK LOCAL
FEC0::/10	UNICAST SITIO LOCAL (RFC 3879)
FC00::/7	Propuesta de UNICAST LOCAL IPv6
FF00::/8	MULTICAST

Direcciones NSAP

- El término PDU (*Protocol Data Unit)* es usado por ISO para todas las capas e incluye a SDU y el encabezado PCI.
- Para cada capa se antepone la inicial a la sigla que la identifica y el nombre más usual:
  - -APDU, PPDU, SPDU: para las capas 7, 6 y 5 respectivamente.
  - -TPDU (capa 4: segmento en TCP y mensaje en SMTP y SS7).
  - -NPDU (capa 3: paquete en X.25 y datagrama en IP).
  - -DPDU (capa 2: tramas en LAN y FR, celda en ATM y MAN y paquete en X.25).
  - -PhPDU (capa 1: trama y envoltura).
- La dirección que identifica la capa se indica como **SAP**
- Da lugar a las direcciones NSAP, DSAP y PhSAP.

Redes

- Una red IPv6 utiliza un grupo de direcciones IPv6 contiguas, de un tamaño potencia de dos.
- La parte inicial de las direcciones son idénticas para todos los hosts de una red, y se llama dirección de red o prefijo de encaminamiento *(routing prefix)*.
- Las direcciones de red se escriben en notación CIDR: una red se representa por la primera dirección del grupo (que debe terminar en ceros), una barra invertida (/), y el número de bits del prefijo en decimal.
- Ejemplo: la red **2001:db8:1234::/48**
  comienza en la dirección **2001:0db8:1234:0000:0000:0000:0000:0000**
  y finaliza en **2001:0db8:1234:ffff:ffff:ffff:ffff:ffff**

Asignación general

- El Internet Architecture Board *(Comité de Arquitectura de Internet)* y el Internet Engineering Steering Group *(Dirección de Ingeniería de Internet)* delegaron la asignación del direccionamiento IPv6 en la Internet Assigned Nubes Authority (IANA).
- Su función principal es la asignación de grandes bloques de direcciones a los Registros Regionales de Internet (RIRs por sus siglas en inglés), que tienen la tarea de asignar trozos menores a Proveedores de Internet u otros registros locales (ISPs).
- IANA ha mantenido la lista oficial de las asignaciones del espacio de direcciones IPv6 desde diciembre de 1995.

- Sólo la octava parte del espacio total de direcciones están disponibles para su uso en Internet.
- La mayor parte de las direcciones IPv6 están reservadas para uso futuro.
- Para conseguir agregación de rutas, reduciendo así el tamaño de las tablas de rutas de Internet, el rango 2000::/3 se asigna a los RIRs en grandes bloques desde /23 hasta /12.
- Los RIRs asignan rangos menores a los ISPs, que luego distribuyen en bloques de /48 a sus clientes..

- Cada RIR puede dividir cada uno de sus bloques /23 en 512 bloques /32, normalmente uno para cada ISP.
- Un ISP puede dividir cada uno de sus rangos /32 en 65.536 bloques /48, normalmente uno para cada cliente.
- Los clientes pueden crear 65.536 redes /64 con su asignación /48, teniendo cada red un número de direcciones que es el cuadrado de todo el espacio de direcciones IPv4, que sólo tenía 2^{32} ó 4.3×10^{9} direcciones.

- Las direcciones IPv6 se asignan a las organizaciones en bloques mucho mayores a las asignaciones IPv4.
- La asignación recomendada es un rango /48, que es 2^{48} ó $2{,}8\times10^{14}$ veces mayor que el direccionamiento IPv4 completo.
- El conjunto total es suficiente para el futuro previsible, pues hay 2^{128} ó sobre $3{,}4\times10^{38}$ direcciones IPv6.

ICMPv6

- ICMPv6 es un protocolo de propósito múltiple diseñado para:
  - detectar errores encontrados en la interpretación de paquetes
  - realizar diagnósticos
  - realizar funciones como Neighbor Discovery
  - detectar direcciones IPv6 multicast.
- Hay dos clases de mensajes
  - mensajes de error
  - mensajes informativos

Tipos de mensajes

- Mensajes de error
  - Destination Unreachable (Destino Inalcanzable)
  - Packet Too Big (Paquete Demasiado Grande)
  - Time Exceeded (Tiempo Agotado)
  - Parameter Problem (Problema de Parámetros
- Mensajes informativos
  - Echo Request (Solicitud de Eco)
  - Echo Reply (Respuesta de Eco)

IPseg - Protocolos

- **Cada host de IPv6 debe soportar al menos dos protocolos de seguridad**, Authentication Header (AH) y Encapsulated Security Payload (ESP) como mecanismos de la capa de seguridad de IP.
- Como la seguridad es parte del diseño del protocolo, debe estar incluidos en todas las plataformas.

-AH provee la integridad y autenticacion del mensaje

-ESP provee confidencialidad e integridad, y autenticacion con el uso de los algoritmos apropiados

- Los mecanismos de seguridad y su manejo poseen una interfase particular denominada SA (Security Association)

IPseg - Modos

Proporciona seguridad en

- **MODO TRANSPORTE** Extremo a extremo del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el procesado de seguridad.
- **MODO TÚNEL** (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

Modo transporte

- Sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada.
- El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash.
- Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP).
- Se utiliza para comunicaciones ordenador a ordenador.
- Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definido por RFCs que describen el mecanismo de NAT transversal.

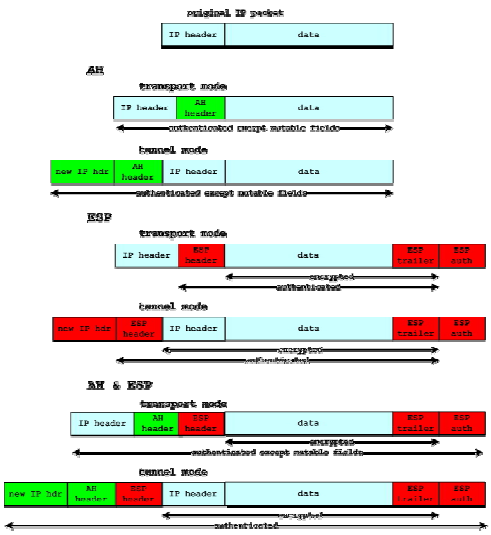
Modo túnel

- Todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado.
- Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento.
- Se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

Protocolos Obligatorios

- **Authentication Header** (AH) proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.
- **Encapsulating Security Payload** (ESP) proporciona confidencialidad y la opción de autenticación y protección de integridad.

Los algoritmos criptográficos definidos para usar con IPsec incluyen HMAC- SHA-1 para protección de integridad, y Triple DES-CBCy AES-CBC para confidencialidad. (RFC 4305).



Authentication Header (AH)

Proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados

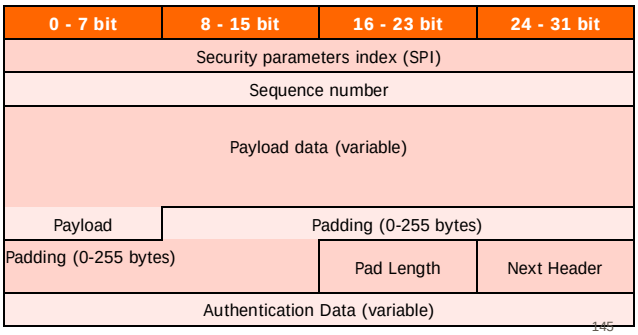
0 - 7 bit	8 - 15 bit	16 - 23 bit
Next header	Payload length	RESERVED
Security parameters index (SPI)		
Sequence number		
Hash Message Authentication Code (variable		

Next header Identifica el protocolo de los datos transferidos.
Payload length Tamaño del paquete AH.
RESERVED Reservado para uso futuro (hasta entonces todo ceros).
Security parameters index (SPI) Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
Sequence number Un número siempre creciente, utilizado para evitar ataques de repetición.
HMAC Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

Encapsulating Security Payload (ESP)

Proporciona confidencialidad y la opción de autenticación y protección de integridad**.**

Puede ser aplicado solo o conjuntamente con AH



- **Security parameters index (SPI)** Identifica los parámetros de seguridad en combinación con la dirección IP.
- **Sequence number** Un número siempre creciente, utilizado para evitar ataques de repetición.
- **Payload data** Los datos a transferir.
- **Padding** Usado para rellenar por completo los bloques.
- **Pad length** Tamaño del relleno en bytes.
- **Next header** Identifica el protocolo de los datos transferidos.
- **Authentication data** datos utilizados para autenticar el paquete.

Ruteo

- Para enviar datos entre redes los routers deben tomar decisiones basadas en el prefijo de la dirección destino
- Cada router tiene una tabla con el rango de direcciones para cada interfaz de salida hacia el próximo router
- Cada tabla tiene un *default router*, al cual se le envían los datos cuyas direcciones no aparecen en la tabla
- Las *host specific route* son direcciones de 32 bits que encaminan datos para determinadas máquinas por determinadas rutas
- Las tablas de ruteo manejan direcciones de red, no direcciones físicas de máquinas
- Siguiendo la nomenclatura original, se usa *gateway* como sinónimo de router

- Los protocolos tienen:
  - Algoritmos para conocer la red y calcular rutas
  - Comandos y respuestas para mensajes
  - Temporizaciones a cumplir
  - Metricas: criterios para medir distancia a una red

- Sistemas terminales y routers mantienen tablas
  - Indican el próximo router al cual mandar datagramas
  - **Estático**: Puede contener rutas alternativas (sistemas chicos)
  - **Dinámico**: Respuesta flexible ante congestión y errores
- Ruteo de fuente
  - La fuente especifica ruta como una lista secuencial de routers
  - Seguridad
  - Prioridad
- Registro de rutas

Criterios de ruteo

- En la Internet original y en las redes chicas todo se resuelve en el núcleo de la red, y los routers utilizan el router default
- En redes grandes se manejan dos criterios:
  - Algoritmo vector distancia:
  - Algoritmo estado de enlaces:

Algoritmo vector distancia

- Utiliza una tabla inicial
- Periódicamente los routers vecinos intercambian información
- Si un router recibe información con menor cantidad de saltos para una red, actualiza su tabla con esa dirección

Algoritmo estado de enlaces

- Por medio de mensajes de broadcast cada router mide la menor distancia a cada red
- La distancia se mide por varios criterios
  - retardo
  - ancho de banda
  - confiabilidad
  - jitter
  - costo

Ruteo interno

- En los host se usa habitualmente el ruteo estático
- En los routers se usa habitualmente el ruteo dinámico
- El ruteo estático es óptimo cuando hay un solo camino para llegar a cada red
- Si hay rutas alternativas, cada AS debe optar por un IGP (*Interior Gateway Protocol*)
- Los IGP habituales son:
  - RIP
  - HELLO
  - OSPF
  - GGP
  - IGRP, EIGRP

GGP

- Fue el primer protocolo de ruteo usado en las redes iniciales
- Hoy no pertenece al conjunto TCP/IP

RIP

- ***Routing Information Protocol:*** originalmente implementado en Unix
- Cuenta el número de saltos
- Supone bajos retardos (tal como una LAN)
- La forma activa la usan los routers y hay actualización periódica porque trasmiten mensajes broadcast
- La forma pasiva la usan los host, sólo recibe información
- Los routers tienen timers escalonados:
  - Mandan información cada 30 seg
  - Refrescan tablas cada 180 seg
  - Borran lo no actualizado cada 120 seg

  De esta forma permiten que se conozcan los problemas

- No considera distancias de más de 15 saltos, por lo que trabaja bien en redes chicas
- La versión 1
  - Soporta múltiples protocolos
  - Usa mensajes UDP
- La versión 2 incluye:
  - Máscaras de subredes
  - Autenticación
  - Mensajes multicast

- Las versiones 1 y 2 soportan IPv4
- La versión ng soporta IPv6
- Historia:
  - Comienza como standard de facto
  - Xerox desarrolla el GWINFO
  - Se lo incluye en Unix (BSD) en 1982
  - En 1988 aparece RFC 1058
- Problemas:
  - Las temporizaciones y el número de saltos demoran el aviso de cambios
  - No puede detectar loops
  - Problemas de algoritmo y de métrica

HELLO

- Protocolo de ruteo que usa el retardo en ms como medida de la distancia a una red
- Como el retardo depende del tráfico, hay cambios en la mejor ruta a lo largo del tiempo
- Utilizado en la NSFNET, ahora está superado
- Funcionaba bien porque esa red tenía seis computadoras DEC y todos los enlaces de igual capacidad

OSPF

- ***Open Short Path First*** : versión Open del Short Path First, desarrollado en 1988
- Usa el algoritmo de estado de los enlaces en una organización jerárquica que se puede dividir en áreas
- Puede balancear carga de enlaces
- Es complejo de administrar
- Tiene varios formatos de mensajes
- Descripto en las RFC 1131 (ver 1) y 1247 (ver 2)
- Cada nodo tiene una base de datos de los enlaces

- LSA: son mensajes o avisos del estado de los enlaces
- Cada router calcula árbol de rutas cada vez que se actualiza la base de datos

IGRP

- Utiliza varios criterios de métrica:
  - Retardo
  - Ancho de banda
  - Confiabilidad
  - Carga del canal
- No está limitado a 15 saltos

EIGRP

- Es una versión mejorada *(Enhanced IGRP)*
- Calcula rutas con otro algoritmo
  - DUAL: *Diffussion Update ALgoritm*
- Soporta VLSM

Ruteo externo

- En las redes grandes es impracticable que todos los router intercambien información
- Hay que agruparlos en áreas de hasta 12 routers
- Los routers fuera de esta área no participan en el protocolo de actualización pero envían los paquetes a la frontera
- Esto puede generar saltos extras, por lo que los router externos deben conocer la configuración de la red
- Detrás de los routers no participantes pueden aparecer redes ocultas que no pueden acceder a todos los destinos

- Un Sistema Autónomo (AS) es el que maneja un administrador, tiene sus propios algoritmos internos y se conecta con otros AS
- Un AS tiene routers
  - —Interiores
  - —De frontera (*border*)

EGP

- EGP (*Exterior Gateway Protocol*) permite que dos AS se intercambien información
- Elimina el problema de las redes ocultas
- El único EGP en servicio es el BGP (*Border Gateway Protocol*) versión 4
- Soporta CIDR
- Cada AS debe designar un router frontera que lo represente
- Soporta actualización de rutas, estado de enlaces (*keep alive*) y autenticación

- Es el único protocolo de ruteo que usa TCP (confiable)
- Tablas tienen direcciones y máscaras que pueden compactarse si hay ceros
- EGP comunica AS con diferente métrica para las mismas rutas, por lo que este dato no se informa hacia fuera
- Lo que se informa son las redes alcanzables, pero sin calificación de los enlaces

Multicasting en Internet

- **Multicast de Hardware**: una forma de broadcast que puede ser aceptado por el NIC o por otros usuarios
- Sus mecanismos son poco eficientes
- **Multicast de Ethernet**: definido por algunos bits de la dirección MAC
- **Multicast en IP**: grupos asignados a una dirección de clase D preasignada o transitoria
- Los host pueden declararse dentro del grupo, pero para enviar mensajes no necesitan pertenecer al mismo
- Direcciones comienzan con 1110
- Rango: desde 224.0.0.0 hasta 239.255.255.255
- Hay direcciones reservadas para todos los sistemas y todos los router

- Multicast en IP puede mapearse en un multicast de Ethernet utilizando los 23 bits menos significativos
- Se usa la dirección $01.00.5E.00.00.00_{16}$
- Ejemplo: 224.0.0.2 pasa a ser $01.00.5E.00.00.02_{16}$
- Los host usan multicast por hardware
- Para controlar el alcance del multicast se hace:
  - — Automático: con el TTl detecta los locales
  - — Por el Administrador
- Los host pueden trabajar en varios modos de multicast:
  - — No enviar ni recibir
  - — Sólo enviar
  - — Enviar y recibir

IGMP

- IGMP (*Internet Group Management Protocol*) es el protocolo usado por los host para avisar que usan multicast
- Los host se adhieren a un grupo específico dentro de una red específica
- En cada red se designa un router para supervisar el grupo
- El router consulta periódocamente (cada 125 seg) si el host aún pertenece al grupo
- Los host responden con un retardo aleatorio para evitar superposiciones
- Todas las comunicaciones usan multicast por hardware
- Las rutas pueden cambiar por el agregado o retiro de un host al grupo

Otros protocolos

- El enrutamiento depende del destino y el origen
- La mayor complicación es que un mensaje multicast puede estar generado por un host que no pertenece al grupo y puede cruzar por redes sin miembros
- Hay dos técnicas para enrutar mensajes:
  - Inundación:
    - Protocolo RPF (*Reverse Path Forwarding*)
    - Ahora se usa TRPF (*Truncated Reverse Path Forwarding*)
  - Árbol:
    - Hay un camino determinado para cada grupo
    - Se utilizan varios protocolos: RPM, DVMRP, CBT, PIM-DM, PIN-SM

- RPM (*Reverse Path Multicasting*) se inunda las redes donde se sabe que hay miembros del grupo
- DVMRP (*Distance Vector Multicast Routing Protocol*) es una extensión del IGMP que se implementa en Unix con el programa *mrouted*
- Cuando debe cruzar una red sin soporte de multicast se hace un túnel encapsulando el datagrama multicast en uno unicast
- CBT (Core Based Trees) propuesto para redes extensas
- Los pedidos de adhesión se almacenan en el core de la red

- Las redes grandes se dividen en áreas, cada una con un core router
- PIM-DM (*Protocol Independent Multicast-Dense Mode*) los routers tienen tablas para el enrutamiento
- Sirve para áreas muy densas, y usa inundación
- PIM-SM (*Protocol Independent Multicast-Sparse Mode*)
- Sirve para redes menos densas e islas de multicast
- Utiliza esquemas de árbol

Conmutación IP

- La conmutación supera en velocidad al direccionamiento de paquetes
- Considera etiquetas y no la dirección de destino
- En redes grandes hay una secuencia de etiquetas
- Es una tecnología orientada a la conexión que puede abarcar un área, no necesariamente la ruta completa
- Conmutación IP:
  - Extraído de la tecnología ATM
  - También llamado conmutación de nivel 3
  - Evoluciona al MPLS (*Multi Protocol Label Switching*)

IP Móvil

- Permite a los host retener la IP original al cambiar de red en forma y transparente a aplicaciones y protocolos
- Cuando un host aparece en otra red se le asigna una IP local y se avisa al router original
- Se establece un túnel entre las dos direcciones haciendo una encapsulación IP-IP
- Estas funciones las realiza un agente extranjero en la red
- Si la red no lo tiene, el host consigue su dirección por DHCP y avisa a su agente local por ICMP
- Esta técnica agrega encapsulación y doble circulación en la red, ya que los paquetes buscan la red de origen