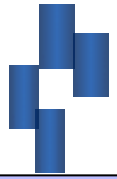
Tema 3
La Capa de Red en Internet

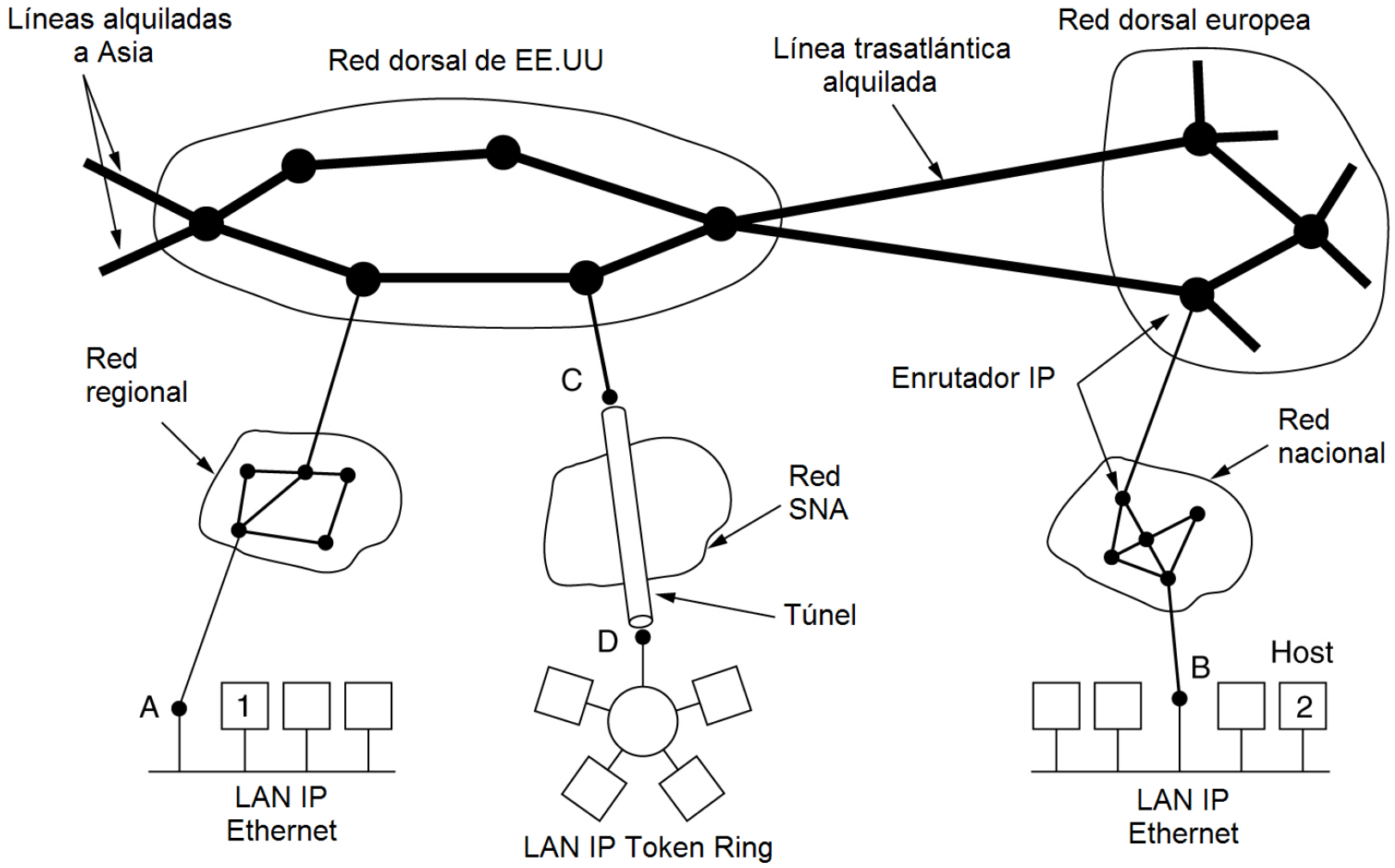
Amelia Zafra Gómez
Dpto. Informática y Análisis Numérico



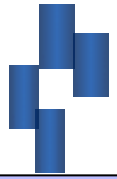
Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

- Internet es un conjunto de subredes o sistemas autónomos interconectados. No hay una estructura real, pero existen varias redes dorsales principales construidas a partir de líneas de alto ancho de banda y enrutadores rápidos.
- Conectadas a las redes dorsales hay redes regionales y conectadas a esta las LANs de muchas Universidades y Empresas.
- El pegamento que mantiene unida a Internet es el protocolo de la capa de red, el Protocolo IP de Internet.



Internet es un conjunto interconectado de muchas redes

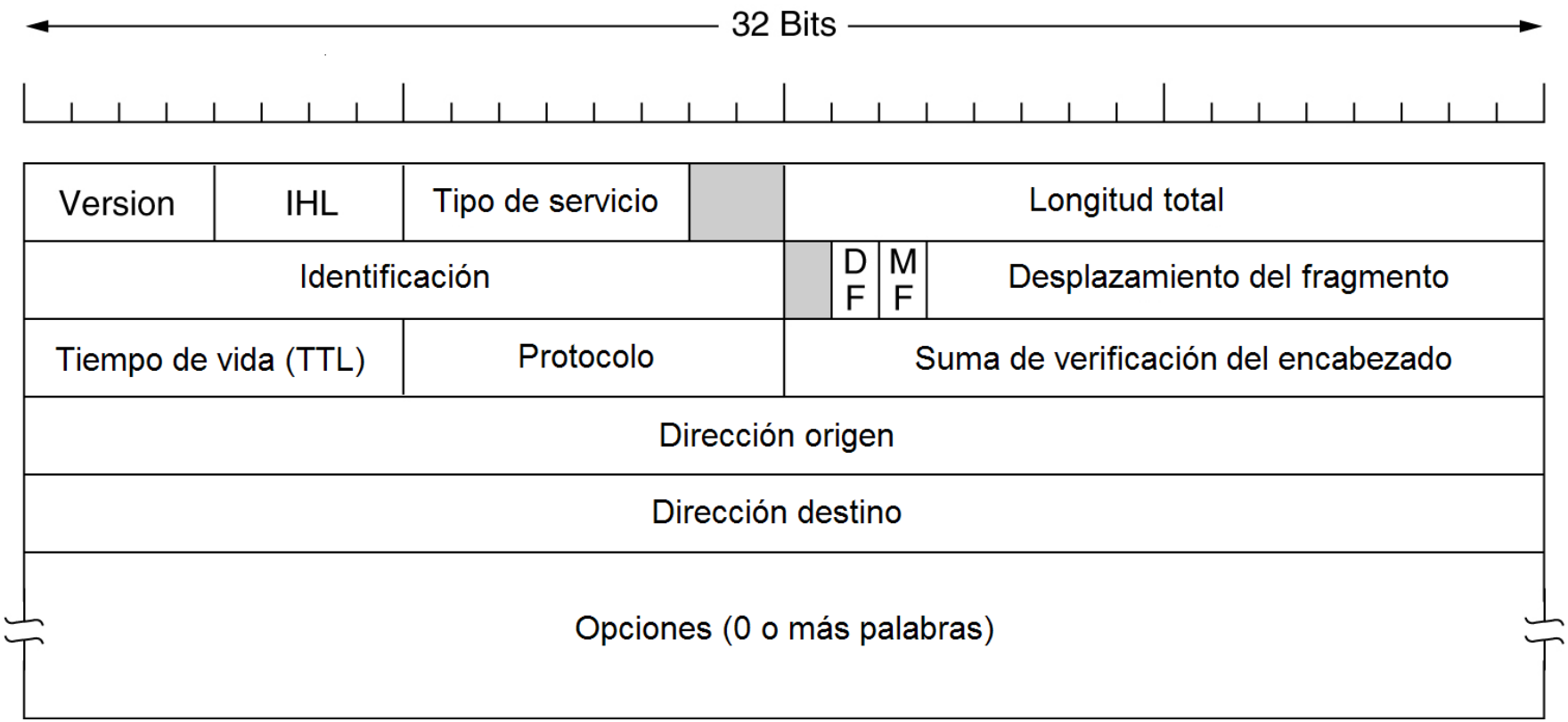


Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

- Desde el principio IP se diseñó con la interconexión de redes en mente.
- Su función es proporcionar un medio de mejor esfuerzo (sin garantías) para el transporte de datagramas del origen al destino, sin importar si las máquinas están o no en la misma red.
- La capa de transporte toma flujo de datos y los divide en datagramas. En teoría los datagramas pueden ser de hasta 64 KB cada uno (se emplean 2 bytes) → en la práctica viene determinado por el tamaño máximo de trama característico de la red utilizada, este tamaño máximo de datagrama se conoce como MTU (Maximum Transfer Unit).
- Así, cuando un datagrama IP llega a un encaminador con un MTU en el enlace de salida inferior al tamaño del datagrama, éste divide el paquete en fragmentos. El reensamblado se realiza en el destino (para llevarlo a cabo se emplean campos del datagrama).

***Recientemente no es del todo cierto → se ha incorporado una serie de mejoras y modificaciones que permiten disponer de Calidad de Servicio en una red IP**



El encabezado de IPv4 (Protocolo Internet).

Un **datagrama IP** consiste en una parte de encabezado y una parte de texto. El encabezado tiene una parte fija de 20 bytes y una parte opcional de longitud variable

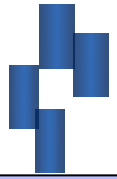
- Versión: lleva el registro de la versión del protocolo (IPv4, IPv6), la 5 fue experimental
- IHL: como la longitud del encabezado no es constante, indica la longitud del mismo en palabras de 32 bits, el valor máximo es 15 (15*4bytes=60 bytes => Opciones tenga 40 bytes).
- Tipo de servicio: indica las clases de servicio basado en prioridades → actualmente se usa para "Servicios Diferenciados" que se encarga de implementar Calidad de Servicio en redes IP.
- Longitud total: longitud de todo el datagrama, incluyendo encabezado y datos, la longitud máxima es 65.535 bytes.
- Identificación: para que el host de destino determine a qué datagrama pertenece un fragmento recién llegado
- DF: no fragmentar el datagrama.
- MF: más fragmentos, todos fragmentos de un datagrama excepto el último tienen este bit activado

- Desplazamiento del fragmento: indica en qué parte del datagrama actual va en este fragmento. Como son 13 bits, puede haber un máximo de 8192 fragmentos por datagrama, que a 8 bytes por fragmento=> 65.536 bytes por datagrama.
- Tiempo de vida (TTL): es un contador que sirve para limitar la vida de un paquete, cuando ha pasado un tiempo excesivo o ha dado un número excesivo de saltos. En la práctica cuenta los saltos, cuando el contador llega a cero, el paquete se descarta.
- Protocolo: indica el protocolo de las capas superiores al que debe entregarse el paquete. Ej., TCP, UDP.
- Suma de verificación: verifica el encabezado, tiene que calcularse en cada salto, pues TTL cambia.
- Dirección de origen y destino: indican el número de red y el número de host de origen y de destino.

- Versión: lleva el registro de la versión del protocolo (IPv4, IPv6), la 5 fue experimental
- IHL: como la longitud del encabezado no es constante, indica la longitud del mismo en palabras de 32 bits, el valor máximo es 15 (15*4bytes=60 bytes => Opciones tenga 40 bytes).
- Tipo de servicio: indica las clases de servicio basado en prioridades → actualmente se usa para “Servicios Diferenciados” que se encarga de implementar Calidad de Servicio en redes IP.
- Longitud total: longitud de todo el datagrama, incluyendo encabezado y datos, la longitud máxima es 65.535 bytes.
- Identificación: para que el host de destino determine a qué datagrama pertenece un fragmento recién llegado
- DF: no fragmentar el datagrama.
- MF: más fragmentos, todos fragmentos de un datagrama excepto el último tienen este bit activado

- Opciones: se diseñó para proporcionar un recurso que permitiera que las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original, así como especificar varias opciones para los datagramas, originalmente cinco opciones:

Opción	Descripción
Seguridad	Especifica qué tan secreto es el datagrama
Enrutamiento estricto desde el origen	Indica la ruta completa a seguir
Enrutamiento libre desde el origen	Da una lista de los enrutadores que no deben evitarse
Registrar la ruta	Hace que cada enrutador agregue su dirección IP (ARPANET 9 enrutadores)
Marca de tiempo	Hace que cada enrutador agregue su dirección IP y su marca de tiempo



Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

- Para hacer un sistema de comunicación universal, se necesita un método de identificar computadoras aceptado globalmente.
- Cada computadora tendrá su propio identificador → conocido como dirección IP.
- Las direcciones IP tienen 32 bits:

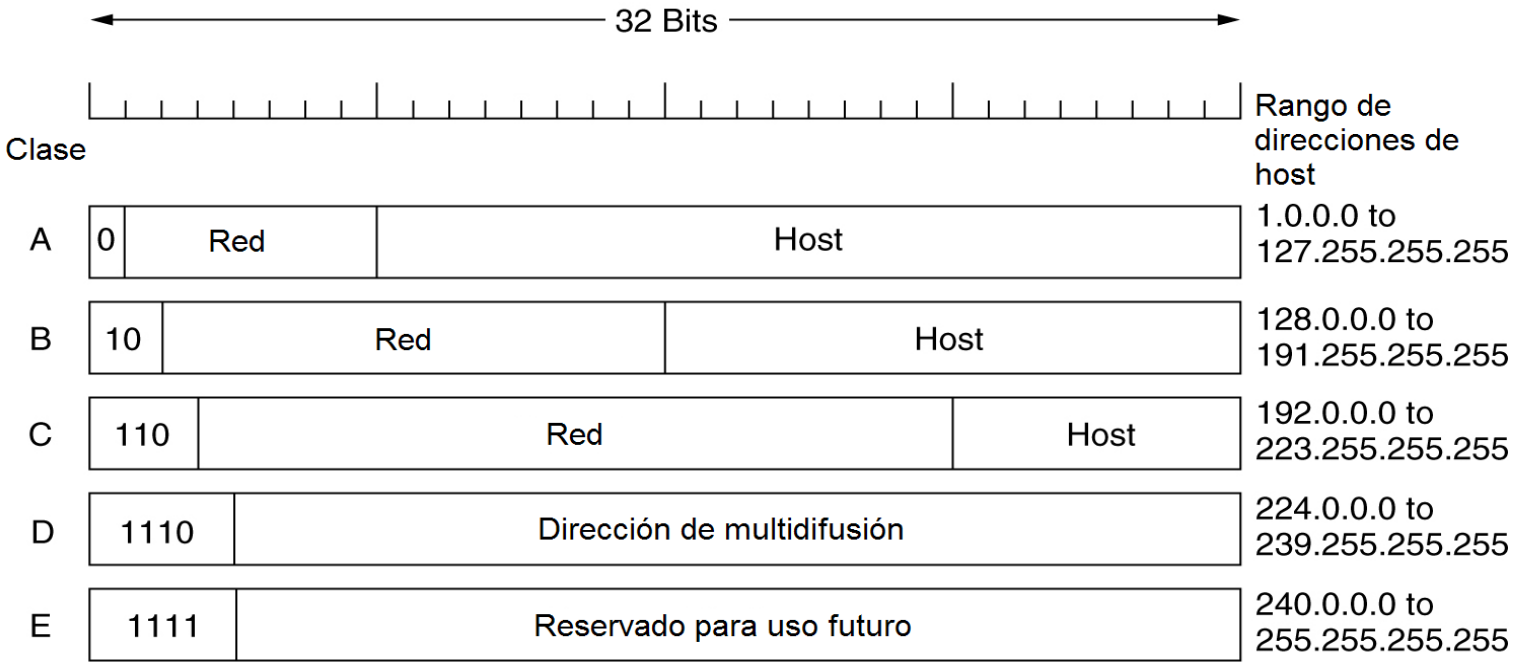
  10000000 00001010 00000010 00011110
- Se suelen representar como cuatro enteros decimales separados por puntos, donde cada entero da el valor de un octeto de la dirección, para facilitar su claridad:

  128.10.2.30
- Cada dirección IP es un par de identificadores (red_id,host_id)

  red_id: identifica una red.

  host_id: identifica a un host dentro de la red.
- Para que se realice una asignación a nivel global de direcciones, existe una organización que se encarga de asignar las direcciones

  ICANN (Corporación de Internet para la Asignación de Nombres y Números)

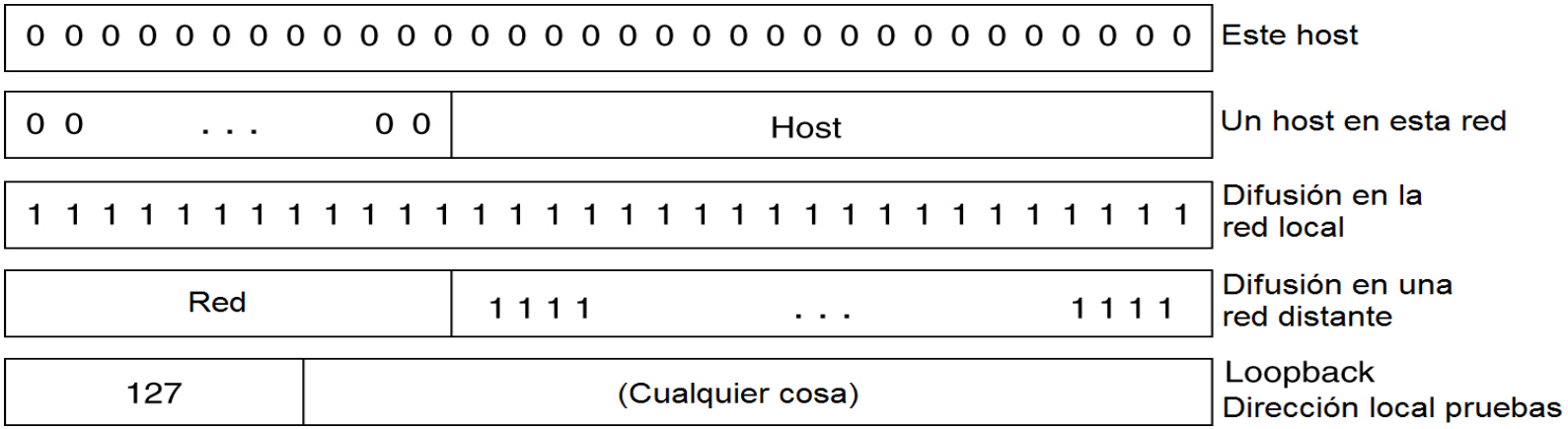


Formatos de dirección IP de 32 bits

Por varias décadas las direcciones IP se dividieron en cinco categorías

A (128 redes con 16777216 hosts cada una), B (16.382 redes con 65536 hosts cada una), C (2097152 redes con 256 hosts cada una), D (para definir grupos multicast, puede haber hasta 268435456 direcciones multicast en Internet), E (las direcciones que comienzan por 1111 se reservan para uso futuro).

Direcciones IP especiales



Existen reglas y convenios que asignan significados especiales a determinadas direcciones IP que es importante conocer

- Las direcciones de red, que son números de 32 bits se escriben generalmente en notación decimal con puntos Ej. 192.41.6.20.
- La dirección 255.255.255.255 se utiliza para indicar broadcast en la propia red. Se utiliza como dirección de destino, no como dirección de origen.
- La dirección 0.0.0.0 identifica al host actual → se utiliza como dirección de origen, no de destino.
- La dirección con el campo red todo a ceros identifica a un host en la propia red, cualquiera que esta sea;

- Las direcciones con el campo host todo a cero identifican redes y por tanto no se utilizan para ningún host. Se emplean para especificar rutas y no deberían aparecer como direcciones de origen o destino de un datagrama.
- La dirección con el campo host todo a unos se utiliza como dirección broadcast dentro de la red y por tanto no se utiliza para ningún host. Se emplea como dirección de destino.

Como consecuencia de estas dos reglas, siempre hay dos direcciones inútiles en una red, la primera y la última. Por ejemplo, si tenemos la red 200.200.200.0 (claseC) tendremos que reservar la dirección 200.200.200.0 para denotar la red misma, y la dirección 200.200.200.255 para envíos broadcast a toda la red; disponemos por tanto en este caso de 254 direcciones para host, no de 256.

- Las direcciones de la clase A 127.0.0.0 se utiliza para pruebas loopback; se interpretan como direcciones del propio host (generalmente 127.0.0.1), devuelven a la dirección de origen los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte).
- Las redes 128.0.0.0, 191.255.0.0, 192.0.0.0 y el rango de 240.0.0.0 en adelante (clase E) están reservados y no deben utilizarse.

Máscaras De Red

- Para indicar qué parte de la dirección corresponde a la red y qué parte al host se suele utilizar las denominadas máscaras.
- Las máscara de red son patrones de 32 bits, consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden al host.
- Cada clase tiene una máscara que identifica la división en red y host que realiza, su representación también se puede realizar en notación decimal con puntos.
- Para cada clase de dirección IP de las estudiadas, su máscara de red sería:
  - Clase A: 255.0.0.0 (8 bits red, 24 hosts).
  - Clase B: 255.255.0.0 (16 bits red, 16 bits hosts).
  - Clase C: 255.255.255.0 (24 bits red, 8 hosts).

Máscaras De Red

- El esquema de direccionamiento IP establece una relación unívoca entre una red física y el identificativo de red IP asociado, reservando el resto de los bits de la dirección IP para indicar un host dentro de la red
  - Ventaja: menos tamaño en las tablas de encaminamiento (entrada por red de destino, en lugar de por host).
  - Inconveniente: con el gran aumento ocurrido en internet, surgen nuevas redes de pequeño tamaño → problema en el espacio de direcciones IP (en lo que respecta a prefijos de red disponibles).
- Para resolver el problema del agotamiento de direcciones IP disponibles hasta que se utilice complementamente la nueva versión, IPv6, que introduce un mayor número de direcciones al considerar 128 bits para la dirección → se han planteado métodos y conceptos para flexibilizar la rigidez que establece las direcciones IP con respecto a la identificación de red y host:
  1. Subredes (subnetting)
  2. Distribución de Redes Privadas
  3. CIDR, superredes (supernetting)

Subredes

- Según el esquema de direccionamiento inicial todos los hosts de una red deben tener el mismo número de red.
- Si por ejemplo una Universidad que inició con una red clase B, utilizada por un Departamento de Informática, se fue ampliando a otros departamentos (localizados en otras LANs) mediante repetidores de la red de Informática, pronto hace falta otra organización (superar el límite de repetidores por Ethernet). Posibilidades:
  - Obtener una 2º dirección de red de clase B: sería difícil debido a que las direcciones de red son escasas y con la dirección que tienen podrían considerar hasta 65534 hosts (considerando las direcciones especiales). El problema es que A, B, C hacen referencia a una red, no a una colección de LANs.
  - Haber considerado para cada red una dirección clase C: esta opción requiere agrupar las redes de la organización ya que cada una sería independiente y sería necesario anunciar en Internet la ruta para cada nueva red para que fuera accesible.
- Conforme más y más organizaciones se encontraron con este problema
  - Se estableció una modificación en el sistema de direccionamiento.

Subredes

- La solución es el empleo de subredes → permite la división de una red en varias subredes (partes) para uso interno, pero actuar como una sola red ante el mundo exterior (no requiere modificar las tablas externas ni una comunicación al ICANN).
- Este esquema permite un mejor aprovechamiento del espacio de direcciones IP → posibilita una mejor estructuración de las redes, en especial de las de clase A y B. Obtenemos un tercer nivel de jerarquización:
  - host: subred + host
- Para implementar subredes, el enrutador principal necesita una máscara de subred que indique la división entre el número de red más el número de subred y el host.
  - Los bits a 1 de la máscara identifican la parte de red y la de subred y los bits a 0 corresponden al host.
- Las máscaras de subred también se pueden escribir en notación decimal separada por puntos 255. 255.252.0 ó agregando a la dirección IP base el número de bits usados para red + subred, separado por una barra. Ej. 194.24.8.0/22

Subredes

- Según el número de bits que se empleen para identificar a la subred y para identificar al host, tendremos mayor número de subredes con menor número de hosts por subred o menor número de subredes con mayor número de hosts por subred.
- De este modo, si empleamos:
  - La máscara 255.255.255.0 en una dirección clase B permitiría 256 subredes de 256 direcciones cada una → convierte una red clase B en 256 subredes clase C.
  - La máscara 255.255.252.0 hace subredes más grandes, reserva los primeros 6 bits para la subred y deja 10 para el host → 64 subredes con 1024 direcciones cada una.

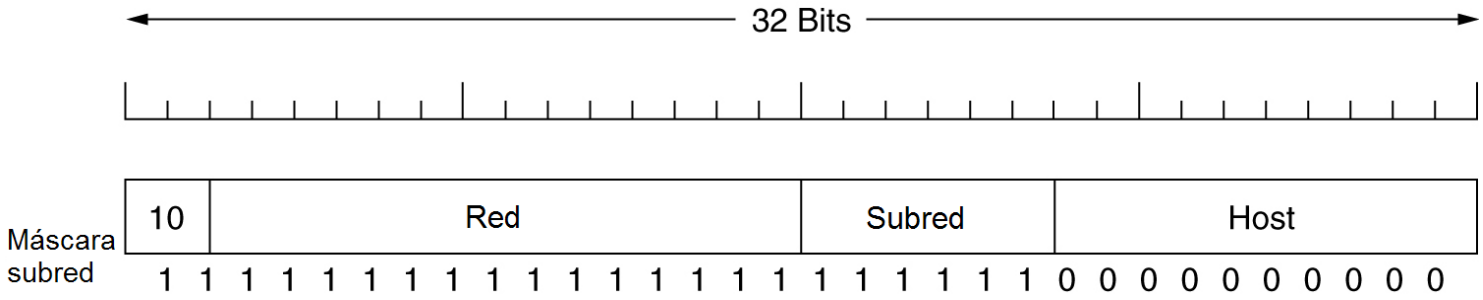


Fig. Una red de clase B dividida en 64 subredes

Subredes

Se debe tener en cuenta que:

- Cuando se crean subredes hay 2 direcciones en cada subred que quedan automáticamente reservadas (tal y como se vio cuando se comentó las direcciones IP especiales)

  - Las que corresponden al host todo a 0s (para indicar la subred)

  - Las que corresponden al host todo a 1s (broadcast den la subred).

- Si la red 156.134.0.0 se subdivide con la máscara 255.255.255.0 se crean 256 subredes del tipo 156.134.subred.host → cada una con 256 direcciones.

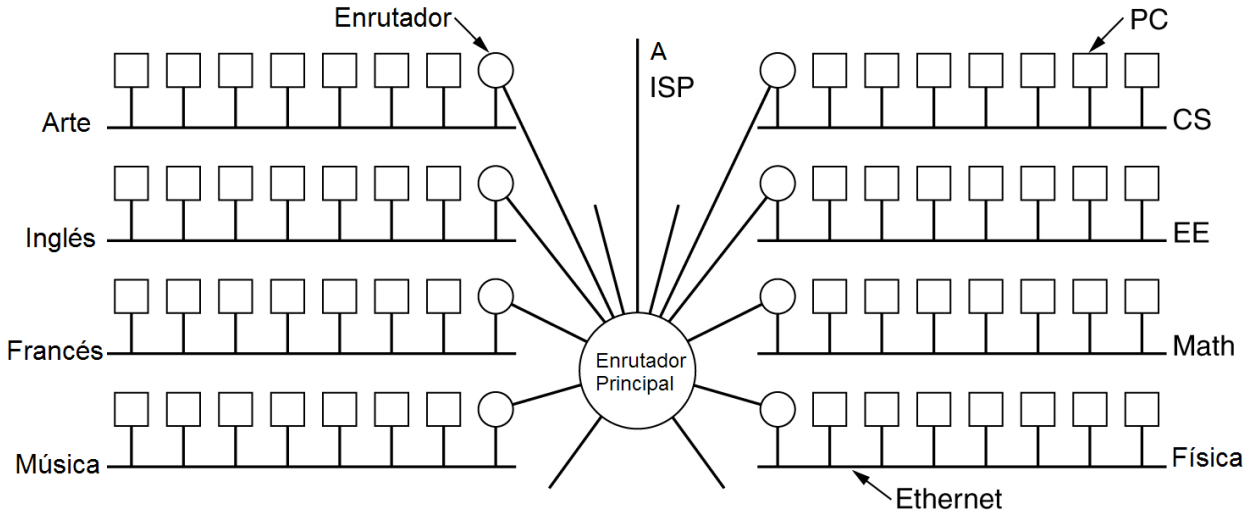
  - En cada subred hay 254 direcciones aprovechables para hosts, ya que la primera dirección (156.134.subred.0) identifica a la subred y la última (156.134.subred.255) es la dirección broadcast de esa subred.

- Igual que los valores todos 0s y todos 1s están reservados con un significado especial en el campo host, con el campo subred ocurre igual (la primera y última subred) también son especiales (*Todo 0s: 156.134.0.0 y Todo 1s:156.134.255.255*)

- Mientras que las restricciones de las direcciones ceros y unos en el host se debe respetar siempre → en el campo de subred se puede violar la restricción y se conoce como subnet-zero y permite aprovechar mejor el espacio de direcciones disponible.

Subredes

- La distribución final del ejemplo de la Universidad propuesto (una red consistente en varias LANs) sería la que se muestra en la figura:

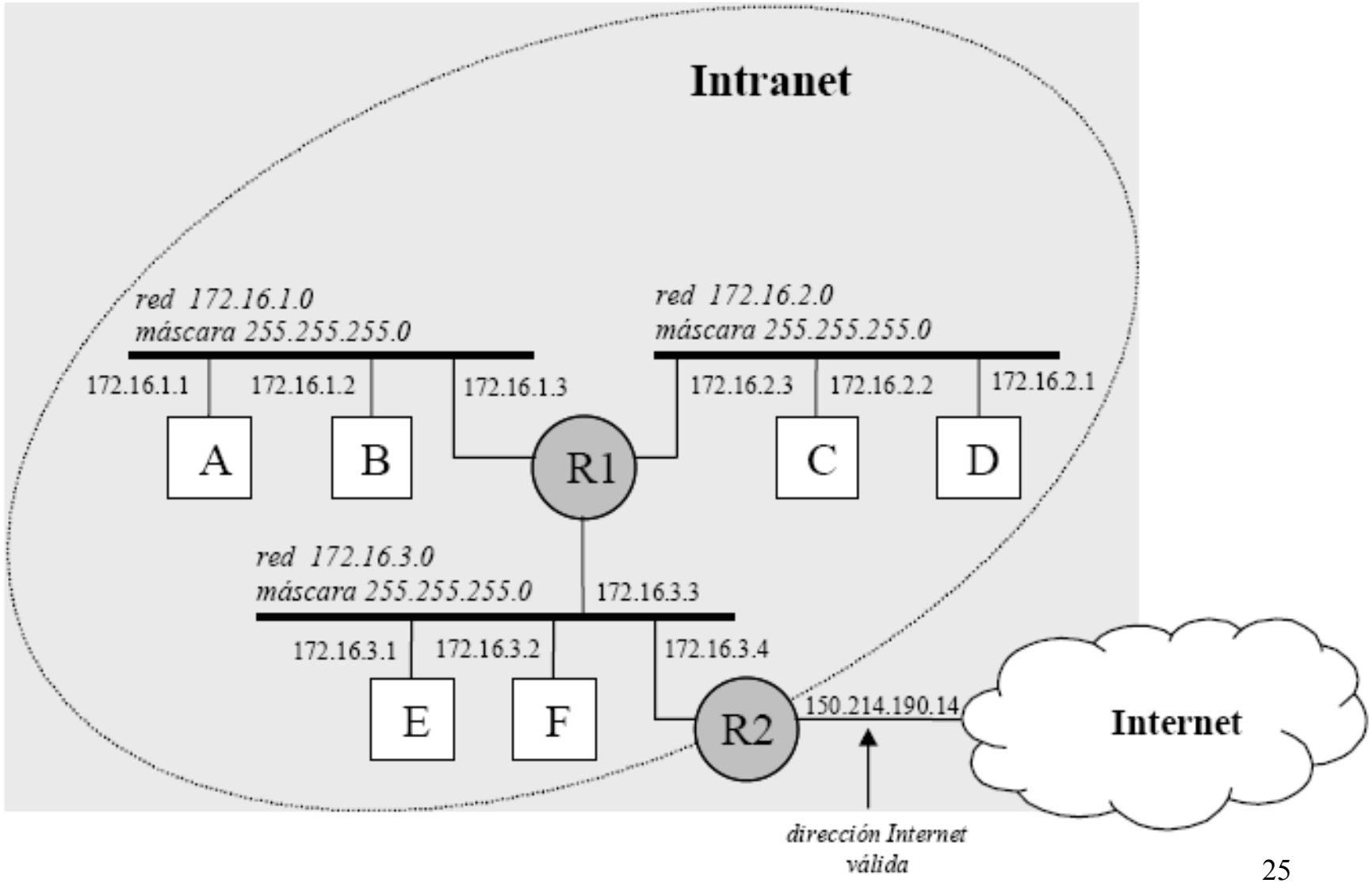


- En lugar de tener una sóla dirección de clase B con 14 bits para el número de red y 16 bits para el número de host, algunos bits se eliminan del número de host para crear un número de subred. Ejemplo: Si la Universidad tiene 35 departamentos, podría utilizar un número de subred de 6 bits y un número de host de 10 bits, lo que permitiría hasta 64 departamentos con 1022 hosts cada una (considerando las direcciones especiales).

Subredes

- Para el ejemplo anterior (/22) podríamos tener una subred 1 que comience en 130.50.4.1, una subred 2 que comience en 130.50.8.1 y una subred 3 que comience en 130.50.12.1
  - Subred 1: 10000010 00110010 000001|00 00000000
  - Subred 2: 10000010 00110010 000010|00 00000000
  - Subred 3: 10000010 00110010 000011|00 00000000
- La barra muestra el límite entre el número de subred y el número de host.
- Cada enrutador tiene una tabla en la que se lista cierto número de direcciones IP (red,0) y cierto número de direcciones IP (esta red, host), para saber cómo llegar a redes distantes y a redes locales respectivamente, lo que evita guardar pares red-host y se reducen las tablas.
- Al introducirse las subredes cambian las tablas agregando entradas con forma (esta red, subred, 0) y (esta red, esta subred, host), para saber cómo llegar a todas las demás subredes y hosts de una subred específica.

Distribución de Redes Privadas



Distribución de Redes Privadas

- Otro enfoque de conservación de direcciones IP se describe en el RFC 1597 "Distribución de redes privadas".
- Permite relajar la regla de que las direcciones IP han de ser unívocas globalmente al reservar parte del espacio de direcciones para redes que se usan exclusivamente dentro de una sola organización y que no requieren conectividad IP con Internet. Hay 3 rangos de direcciones reservadas para este propósito:
  - **10.0.0.0 a 10.255.255.255/8 (1 red clase A)**
  - **172.16.0.0 a 172.31.255.255/12 (16 redes clase B)**
  - **192.168.0.0 a 192.168.255.255/16 (256 redes clase C)**
- Cualquier organización puede usar cualquiera de estos rangos → pero al no ser unívocas a nivel global no pueden ser direccionadas por hosts de otras organizaciones y no están definidas para los routers externos.
- Para que un paquete proveniente de una red privada pueda ser enrutado al exterior de dicha red hay que traducir la dirección de origen (una dirección IP privada) a una dirección IP pública → dos mecanismos que logran esto son NAT y PAT.

Distribución de Redes Privadas

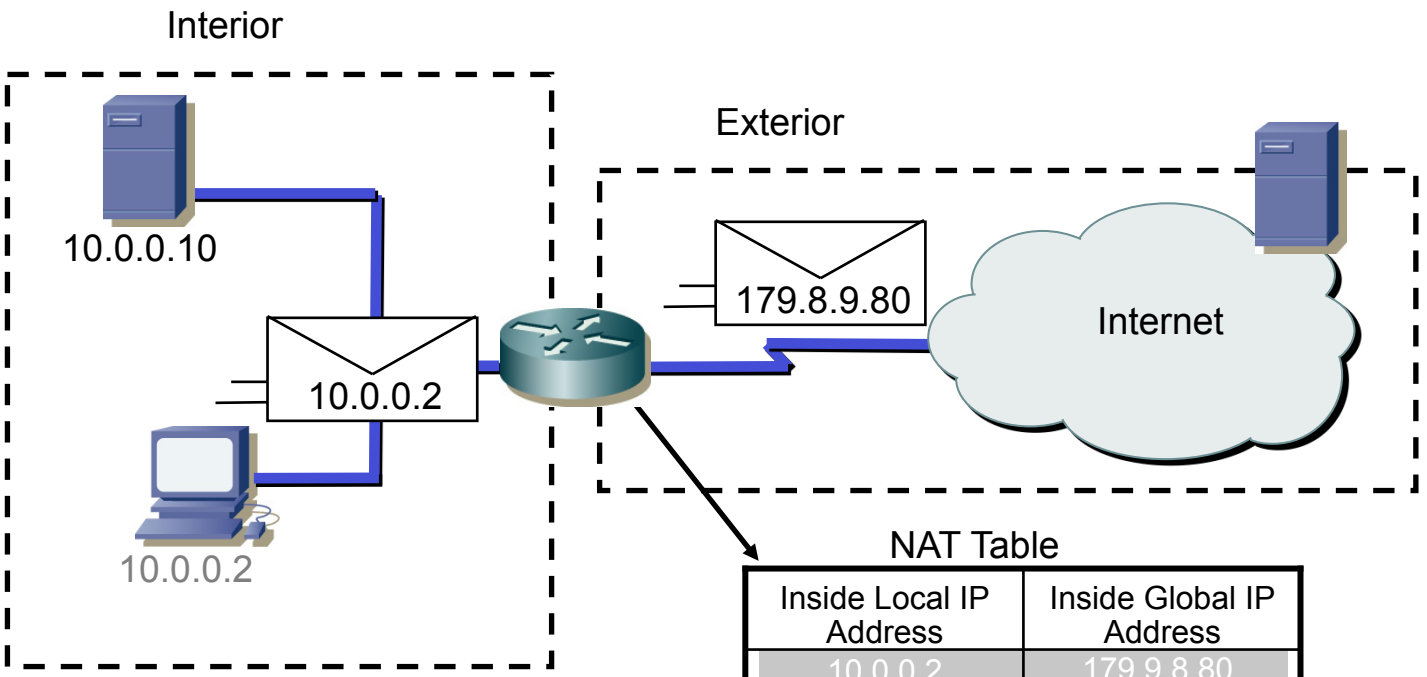
NAT: Traducción de Dirección de Red

- La Traducción de Direcciones de Red (NAT o *Network Address Translation*) es un mecanismo que permite traducir una dirección IP privada a una pública de forma que los paquetes pertenecientes a un host puedan ser enrutados.
- Cuando un host dentro de una red desea hacer una transmisión a un host en el exterior, envía el paquete al router del gateway fronterizo.
- El router del gateway fronterizo realiza el proceso de NAT, traduciendo la dirección privada interna de un host a una dirección pública, enrutable y externa.
- Existen dos tipos de NAT:
  - **NAT estática:** utilizada para servidores de empresas o dispositivos de networking. Cada dirección IP privada se asocia con una sola dirección IP pública específica.
  - **NAT dinámica:** utilizada para los hosts. Cada dirección IP privada se asocia a una dirección IP pública dentro de un conjunto de direcciones IP públicas disponibles.

Distribución de Redes Privadas

NAT: Traducción de Dirección de Red

- El siguiente es un ejemplo del uso de NAT



NAT Table

Inside Local IP Address	Inside Global IP Address
10.0.0.2	179.9.8.80
10.0.0.10	179.9.8.10

Distribución de Redes Privadas

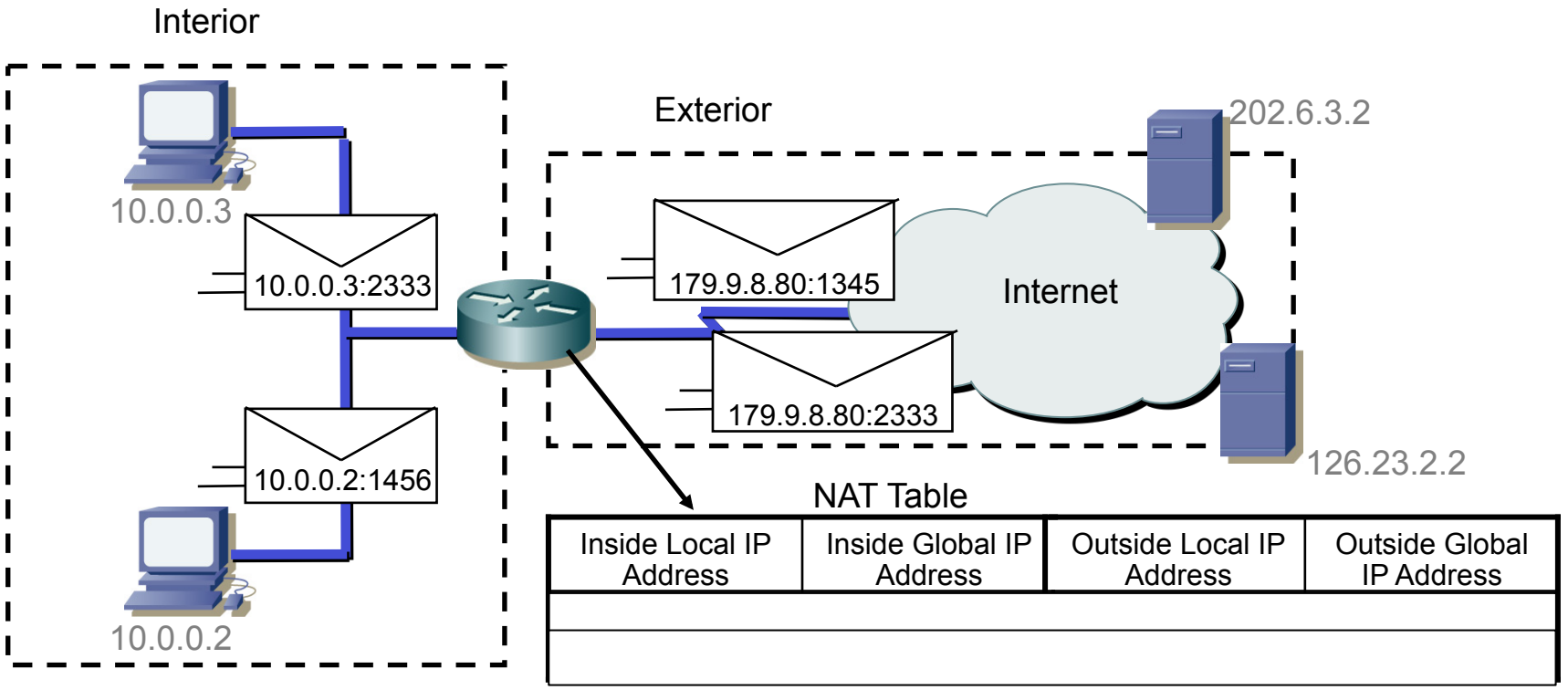
PAT: Traducción de Dirección de Puertos

- Una técnica relacionada con NAT dinámica es la Traducción de Direcciones por Puerto (PAT), también conocida como sobrecarga de direcciones públicas.
- PAT asocia varias direcciones IP privadas a una sola dirección IP pública, asignándole a cada host un número de puerto.
- Cuando se hace una traducción, PAT intenta asignarle a la dirección IP pública el mismo número de puerto que se le asignó a la dirección IP original (la privada).
- Si el número de puerto original está en uso, PAT asigna el primer número de puerto disponible comenzando desde el principio del grupo de puertos correspondiente 0-511, 512-1023, o 1024-65535.
- En teoría, el número total de direcciones internas que se pueden traducir a una sola dirección externa podría ser hasta 65,536 por dirección IP.
  - En realidad, el número de puertos que se pueden asignar a una sola dirección IP es aproximadamente 4000.
- 'IP masquerade o enmascaramiento o NAPT (Network Address Port Translation).' → es el nombre que recibe un tipo de traducción de direcciones de red que permite que todas las máquinas de una red privada utilicen Internet contando con una única conexión (y una única dirección IP).

Distribución de Redes Privadas

PAT: Traducción de Dirección de Puertos

- El siguiente es un ejemplo del uso de PAT:



Distribución de Redes Privadas

- NAT y PAT ofrecen las siguientes ventajas:
  - NAT y PAT permite conectar redes privadas a Internet, sin tener tantas direcciones como host formen la red.
  - NAT y PAT protege la seguridad de la red ya que las redes externas no conocen las direcciones privadas de los hosts de la red interna.
  - PAT conserva las direcciones mediante la multiplexión a nivel de puerto de la aplicación. Con PAT, los hosts internos pueden compartir una sola dirección IP pública para toda comunicación externa.
- Problemas con NAT :
  - Permitir la traducción de direcciones causa una pérdida en la funcionalidad.
  - NAT aumenta el retardo debido a la traducción.
  - Una desventaja significativa que surge al implementar y utilizar NAT, es la pérdida de la posibilidad de rastreo IP de extremo a extremo.

CIDR: Enrutamiento interdominios sin clases

- Problema: agotamiento del espacio de direcciones IP.
  - El sistema de clases original desaprovecha gran cantidad de direcciones cuando una determinada organización se le asigna la clase A o B y utiliza un porcentaje mínimo de ellas.
  - Existen menos de 17 mil direcciones de clase B (más solicitadas) y más de 2 millones de clase C (menos solicitadas).

- Solución: asignar grupos de clases C a una organización.
  - Que las organizaciones puedan optar por niveles intermedios entre la clase B y C, más adecuados a sus necesidades.
  - Si una organización necesita 2000 direcciones se le asigna 8 redes de clase C, en vez de una dirección clase B, con la que no se aprovecharía todas las direcciones que permite la clase B (hasta 65,535 direcciones permitidas).

CIDR: Enrutamiento interdominios sin clases

- Nuevo problema: explosión de las tablas de rutas.
  - Una red de clase B de 3000 host requiere una entrada en la tabla de encaminamiento para cada "router" troncal, pero si la misma red se direccionase como un rango de redes de clase C, requiere una entrada diferente para cada red asignada, requeriría por tanto 16 entradas.
  - Esto ocasiona un problema de crecimiento exponencial en las tablas de rutas, aumento no lineal en la complejidad de los algoritmos relacionados con el mantenimiento de tablas, en general todo el diseño del software en los enrutadores no fue pensado para ese tamaño.
- Nueva solución: considerar un grupo contiguo de redes clase C como una sola red. Hacer superredes.
  - Ampliada al resto del espacio de direcciones a esta técnica se le denomina CIDR (Classless inter Domain Routing).
  - Este sistema extiende las máscaras de red de forma que una dirección de red y máscara de subred puedan especificar varias subredes de clase C.

CIDR: Enrutamiento interdominios sin clases

ENCAMINAMIENTO EN CIDR

- No encamina de acuerdo a la clase del número de red sino sólo según los bits de orden superior de la dirección IP: prefijo IP.
- Cada entrada de encaminamiento CIDR contiene una dirección IP de 32 bits y una máscara de red de 32 bits, que en conjunto dan la longitud y valor del prefijo IP
  - Se le llama supernetting (super-redes) porque el encaminamiento se basa en máscaras de red más cortas que la máscara de red natural de la dirección IP, en contraste con el subnetting (sub-redes) , donde las máscaras de red son más largas que la máscara natural.
  - A diferencia de las máscaras de subred, que normalmente son contiguas pero pueden tener una parte local no contigua, las máscaras de superred son siempre contiguas
- CIDR maneja el encaminamiento para un grupo de redes con un prefijo común con una sola entrada de encaminamiento.

CIDR: Enrutamiento interdominios sin clases

EJEMPLO CIDR

- Si se necesitan 1000 direcciones → no se pide una red de clase B (que se están agotando y de las que se desaprovecharía 64.535 direcciones). con CIDR juntaríamos 4 subredes de la clase C.

```
192.60.128.0      (11000000.00111100.10000000.00000000) Dirección clase C
192.60.129.0      (11000000.00111100.10000001.00000000) Dirección clase C
192.60.130.0      (11000000.00111100.10000010.00000000) Dirección clase C
192.60.131.0      (11000000.00111100.10000011.00000000) Dirección clase C
-------------------------------------------------------------------------------------------
192.60.128.0      (11000000.00111100.10000000.00000000) Dirección de la superred
255.255.252.0     (111111111.11111111.11111100.00000000) Máscara de subred
192.60.131.255    (11000000.00111100.10000011.11111111) Dirección de broadcast
```

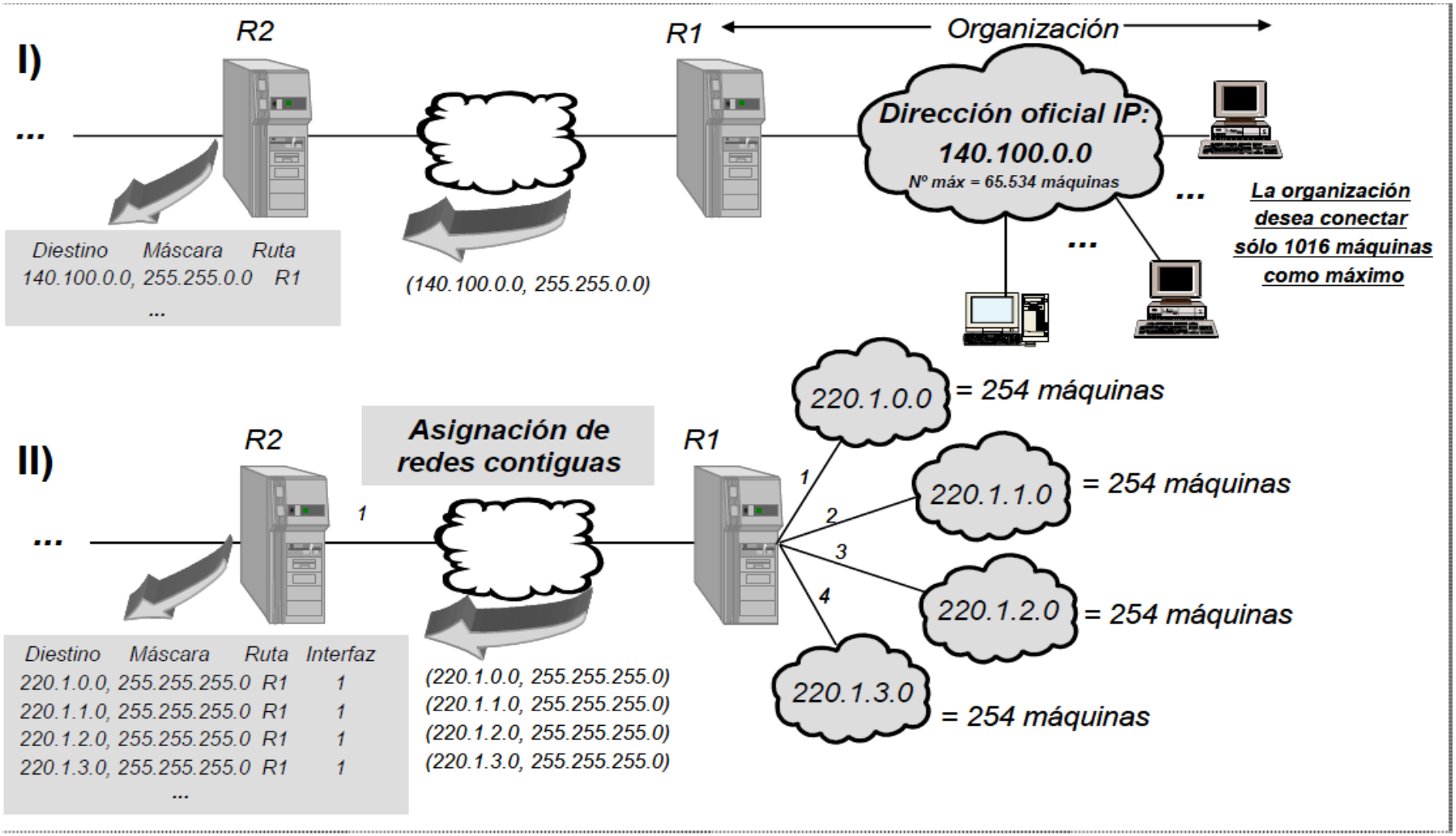
CIDR: Enrutamiento interdominios sin clases

EJEMPLO CIDR

- En este ejemplo se modifica las máscara para que con una entrada a la subred 192.60.128.0 se incluyan todas las direcciones desde 192.60.128.0 hasta 192.60.131.255
  - La máscara de subred muestra que la parte de la dirección que representa a la red tiene 22 bits de longitud (bits 1 de la máscara) y la parte que representa al host tiene 10 bits de longitud (bits 0 en la máscara).
    - Dos formas de representarla
      - 192.60.128.0/22 (lo que indica que hay 22 bits a 1 en la máscara)
      - 192.60.128.0 con máscara 255.255.252.0.

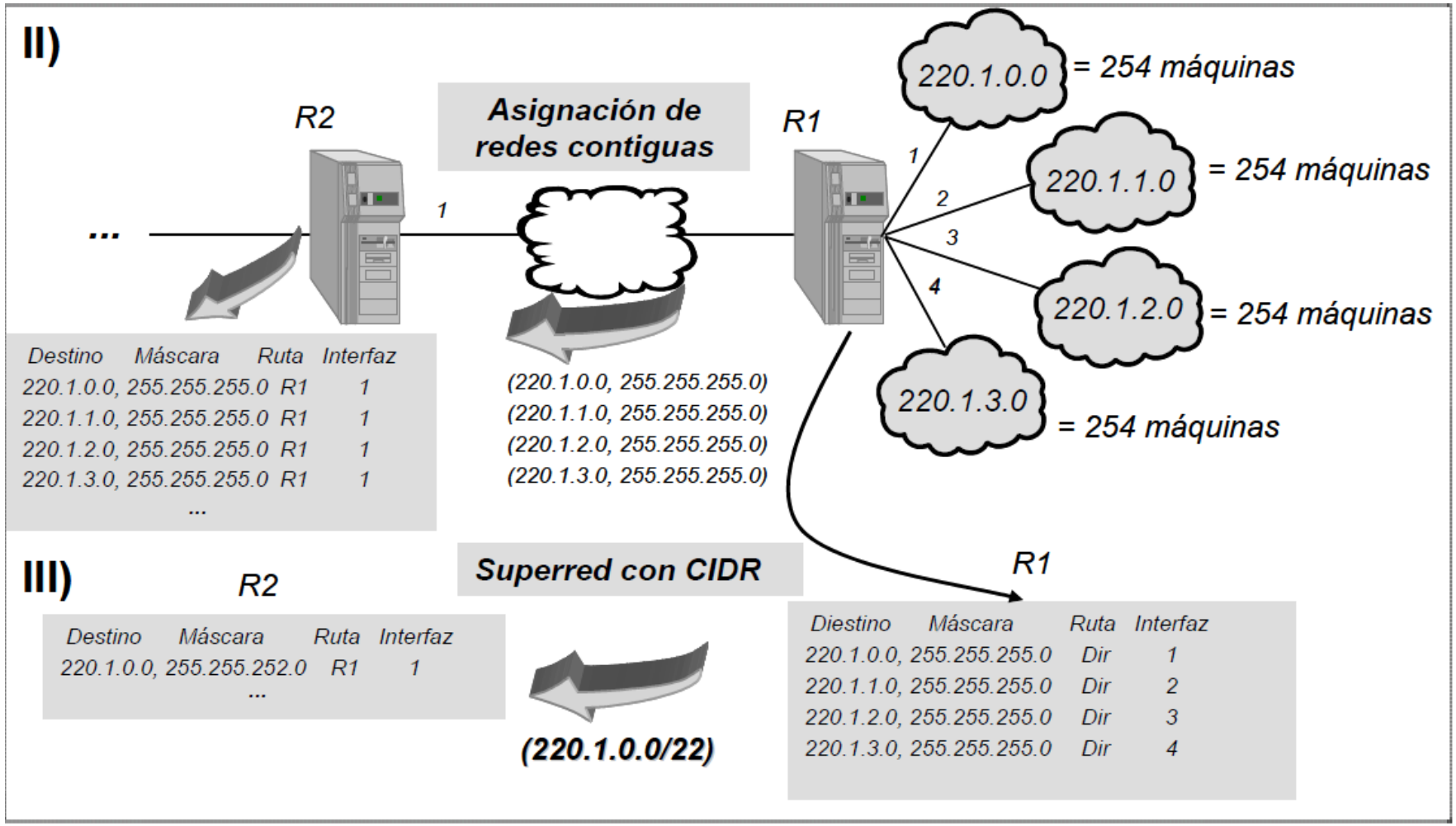
CIDR: Enrutamiento interdominios sin clases

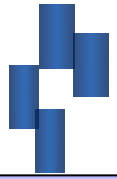
EJEMPLO CIDR



CIDR: Enrutamiento interdominios sin clases

EJEMPLO CIDR





Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

- Además de IP que se usa para la transferencia de datos, Internet tiene algunos protocolos de control que se usan en la capa de redes:

  - ICMP: Protocolo de mensajes de Control en Internet
  - ARP: Protocolo de resolución de direcciones
  - RARP: Protocolo de resolución inversa de direcciones.
  - BOOTP: Protocolo de resolución inversa de direcciones.
  - DHCP: Protocolo de resolución inversa de direcciones.

Protocolo ICMP

- Los enrutadores supervisan estrechamente el funcionamiento de Internet. Cuando ocurre algo inesperado ICMP informa del evento. Hay definidos una docena de tipos de mensajes ICMP:
  1. Destino inalcanzable: No pudo entregarse el paquete.
  2. Tiempo excedido: TTL de un paquete llega a cero.
  3. Problema de parámetro: Campo de cabecera no válido.
  4. Control de congestión: paquete regulador.
  5. Reenvío: Enseña a un enrutador mejores rutas.
  6. Eco: Pregunta a una máquina si está viva.
  7. Repuesta Eco: Sí estoy viva.
  8. Solicitud de timestamp: Igual que el eco pero marcando el tiempo.
  9. Respuesta timestamp: igual respuesta eco pero con tiempo.

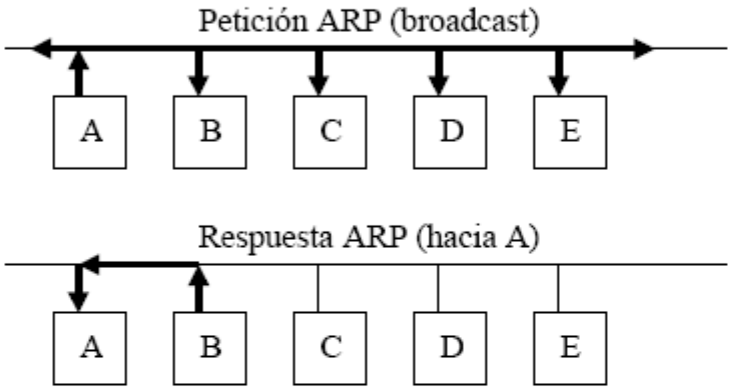
Protocolo ARP

- Este protocolo se utiliza en las redes locales para enviar paquetes de una máquina a otra debido a que el hardware de la capa de enlace de datos no entiende de direcciones IP, por lo que es necesario una conversión de dirección IP a dirección MAC.

- Una solución es tener un archivo de configuración en alguna parte del sistema que relacione IP con direcciones Ethernet. Para las organizaciones con miles de máquinas, conservar todos estos archivos actualizados propicia errores y consume mucho tiempo.

Protocolo ARP

- La idea del ARP es la siguiente
  1. Cuando un "host A" desea comunicarse con otro B, del que conoce su dirección IP (IB), pero no su dirección física (FB).
  2. Envía un paquete especial con dirección de destino broadcast, pidiendo al "host" que tiene como dirección IP IB que responda con su dirección física FB.
  3. Todos los "hosts" conectados a la red reciben el paquete ARP, pero sólo el "host" B, que es al que iba dirigida la pregunta, responde con otro paquete ARP, enviando su dirección física.



Protocolo ARP

- Se pueden hacer varias optimizaciones para que ARP funcione con más eficiencia y es guardar el resultado de la correspondencia en una caché, de este modo, si tiene que comunicarse en poco tiempo con el mismo host evitar una segunda difusión → la experiencia demuestra que merece la pena mantener una tabla dinámica en la memoria volátil con las direcciones IP y las correspondientes direcciones físicas con las que se ha establecido comunicación más recientemente, porque normalmente, la comunicación requiere el envío de varios paquetes.

- Esta caché debe expirar en unos cuantos minutos, para permitir que las correspondencias cambien. Ej. Fallo de una tarjeta ethernet.

- Otra optimización es que cada máquina difunda su correspondencia IP-MAC cuando arranca, así cada máquina que reciba el mensaje lo puede incluir en su caché.

Protocolo RARP

- ARP resuelve el problema de encontrar qué dirección Ethernet corresponde a una dirección IP. A veces se tiene que resolver el problema inverso. En particular esto ocurre cuando se inicializa una estación de trabajo sin disco duro, en este caso puede conocer su MAC (dirección de Ethernet), pero no su IP.
- La solución fue RARP. Este protocolo permite que una estación de trabajo recientemente inicializada transmita su dirección Ethernet y diga:

  - Mi dirección Ethernet es tal. ¿Alquien allá fuera conoce mi dirección?

  - El servidor RARP ve esta solicitud y busca la dirección Ethernet en sus archivos de configuración y devuelve la IP correspondiente.

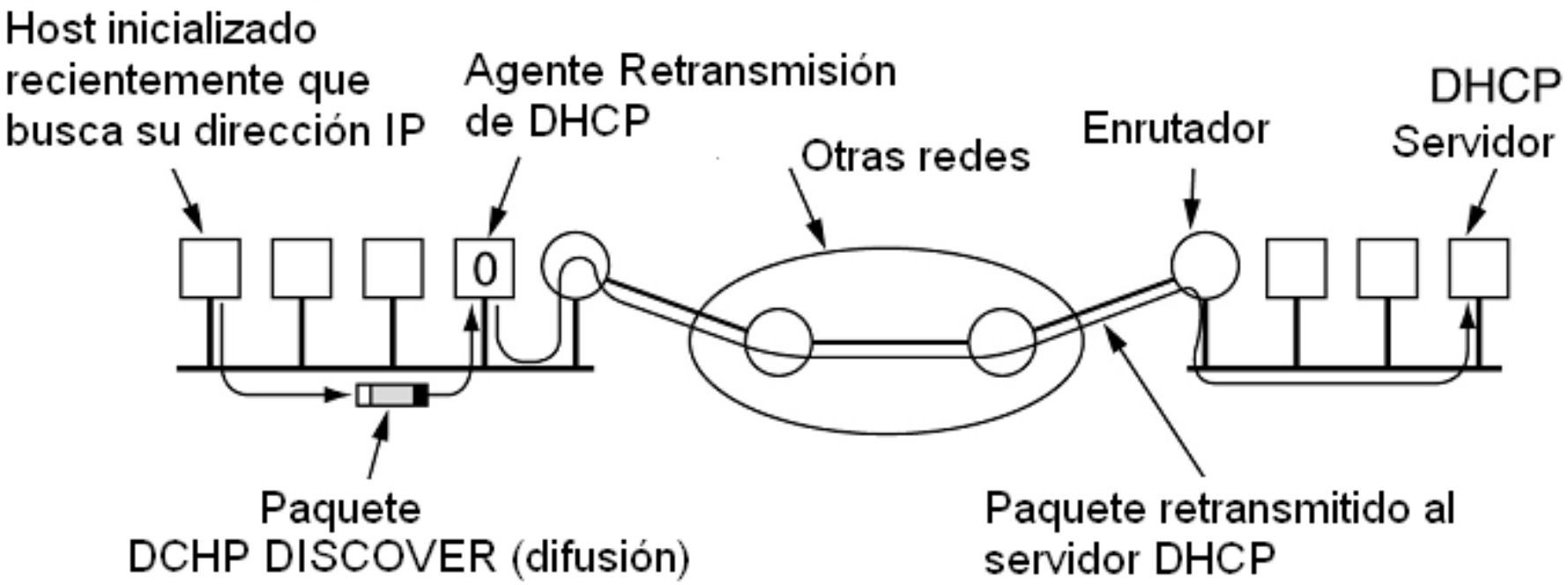
Protocolo BOOTP

- Una desventaja de RARP es que usa una dirección de difusión para llegar al servidor RARP, estas difusiones no las envían los enrutadores por lo que es necesario tener un servidor RARP en cada red local.
  - Para resolver este problema se inventó un protocolo de arranque alternativo (BOOTP), que usa mensajes UDP que se envían a través de los enrutadores.
- BOOTP, descrito en el RFC 951, funciona sobre un datagrama UDP encapsulado sobre IP, que se envía a la dirección de difusión. El servidor de BOOTP recibe ese paquete y devuelve la respuesta con la dirección MAC.
- BOOTP proporciona además de la dirección IP, información adicional a la estación, como puede ser la dirección del servidor DNS, la máscara de subred y la dirección del enrutador predeterminado, para que de este modo pueda realizar la configuración IP.
- BOOTP tiene la desventaja de que requiere una configuración manual de las tablas para relacionar una dirección IP con una MAC. No fue diseñado para direccionamiento dinámico en sus orígenes.
  - Cuando un cliente solicita una dirección IP, el servidor BOOTP busca una entrada en una tabla predefinida que coincida con la dirección MAC del cliente. En caso de que exista dicha entrada, la IP correspondiente es devuelta al cliente. Esto significa que el enlace entre las direcciones MAC e IP se tiene que haber configurado previamente en el servidor BOOTP.

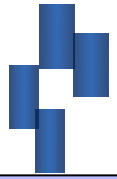
Protocolo DHCP

- DHCP descrito en el RFC 2131, es una extensión de BOOTP, permite tres mecanismos para asignar una dirección IP al cliente:
  - Asignación automática: DHCP asigna una dirección IP permanente a un cliente.
  - Asignación manual: el administrador asigna la dirección IP del cliente y DHCP se la comunica.
  - Asignación dinámica: DHCP asigna una dirección IP al cliente durante un período limitado de tiempo (alquiler).
- Como RARP y BOOTP se basa en la idea de un servidor especial que asigna direcciones IP a hosts que lo requieren.
- El servidor DHCP no necesita estar en la misma LAN, en cuyo caso cada LAN dispondrá de un agente de retransmisión DHCP, que se encargue de mandar el paquete al servidor DHCP.
- Permite asignación dinámica para ello define mecanismos a través de los cuales los clientes pueden estar asignados a una dirección IP por un período de alquiler finito (permitiendo más adelante la reasignación de la misma a otro cliente) o asignándole otra nueva en caso de que se traslade a una nueva subred. Los clientes pueden renovar los alquileres y mantener la misma dirección IP.

Protocolo DHCP



Funcionamiento de DHCP. Para alcanzar su dirección IP, una máquina inicializada recientemente difunde un paquete DHCP DISCOVER. El agente de su LAN (que contiene la IP del servidor DHCP) intercepta todas las difusiones DHCP y lo envía al servidor DHCP, quien nos devolverá la dirección IP y otros parámetros de configuración.



Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

Protocolos de Enrutamiento en Internet

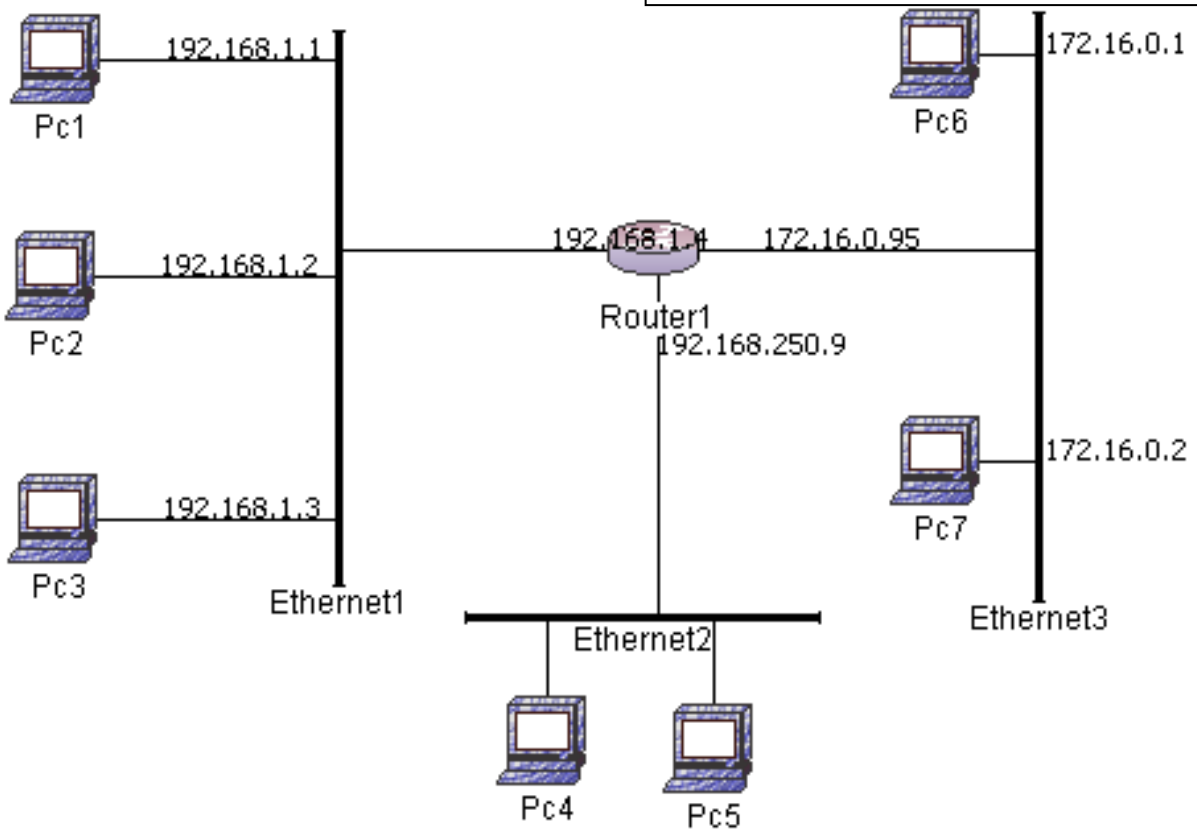
Dado un datagrama IP, el proceso de encaminamiento seguido para su transmisión en cada uno de los nodos intermedios de la subred es el siguiente:

1. Extracción de la dirección IP de destino especificada en el datagrama, IP_D.
2. Para cada entrada en la tabla de encaminamiento, consistente en un identificativo de red de destino (IP_N) y la máscara asociada (M_N), además del siguiente nodo en la ruta a seguir hasta dicha red, se procede como sigue:
    a. Se lleva a cabo la operación lógica AND, bit a bit, entre IP_D y la máscara de red, obteniéndose el identificativo de red IP_R.
    b. Si $IP_N = IP_D$ dicho paquete se encaminará como se indica en la tabla, tomando como dirección física (MAC) de destino la del siguiente dispositivo de encaminamiento en la ruta.
    c. Si $IP_N <> IP_D$ se procede a consultar la siguiente entrada en la tabla.

Protocolos de Enrutamiento en Internet

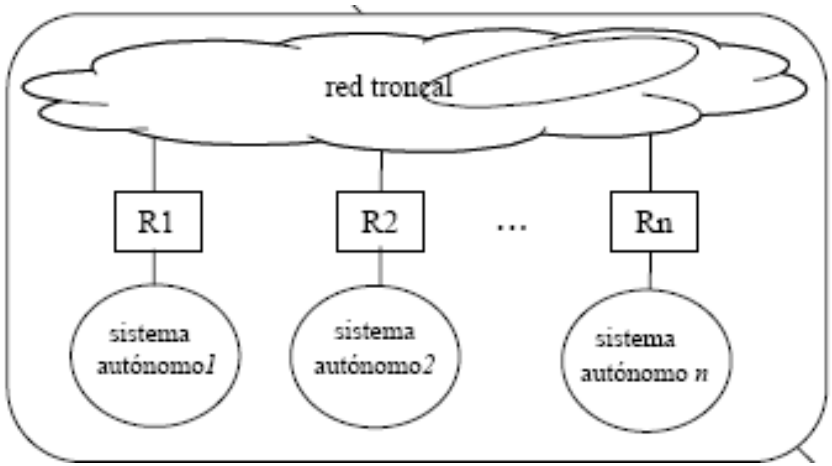
3. Si tras la consulta de toda la tabla no se encuentra coincidencia alguna, se elegirá una ruta por defecto. Si ésta no existe se generará una situación de error (mensaje ICMP).

Pc3 quiere mandar un mensaje a 172.16.0.1



Protocolos de Enrutamiento en Internet

- Para facilitar la administración y aumentar la escalabilidad Internet se jerarquiza en **Sistemas Autónomos** (SA).
- Un SA es un conjunto de subredes, y el hardware asociado, administradas por una única autoridad, de forma que en ella se puede implementar un algoritmo de encaminamiento independientemente de los considerados en otros sistemas autónomos.



Protocolos de Enrutamiento en Internet

- Dos niveles de encaminamiento
  1. **Un algoritmo de enrutamiento dentro de un sistema autónomo** se llama protocolo de enrutamiento de puerta de enlace interior (IGP).
  2. **Un algoritmo para enrutamiento entre sistemas autónomos** se llama protocolo de enrutamiento de puerta de enlace exterior (EGP).
- El protocolo IGP de Internet el administrador tiene libertad de elección, aunque se suele optar por la opción recomendada. Originalmente era RIP (protocolo de vector distancia) basado en Bellman-Ford hasta 1979 que se sustituyó por el protocolo de estado del enlace.
- En 1998 se empezó a trabajar en su sucesor llamado **OSPF (Abrir primero la ruta más corta).**

Protocolo OSPF

- OSPF en 1990 se convirtió en norma y la mayoría de los vendedores de enrutadores lo apoyan. Para su diseño se establecieron una serie de requerimientos:
  1. Tenía que publicarse en código abierto.
  2. Tenía que apoyar una variedad de métricas de distancia: como distancia física, retardo,etc.
  3. Tenía que ser un algoritmo dinámico que se adaptara rápidamente a los cambios de topología.
  4. Tenía que apoyar el enrutamiento en base al tipo de servicio.
  5. Tenía que balancear la carga en múltiples líneas, los anteriores protocolos sólo tenían en cuenta la mejor, no la segunda mejor, lo que mejora el desempeño.
  6. Se necesitó mejorar el sistema jerárquico.
  7. Seguridad (autentificación y privacidad).

Terminología OSPF

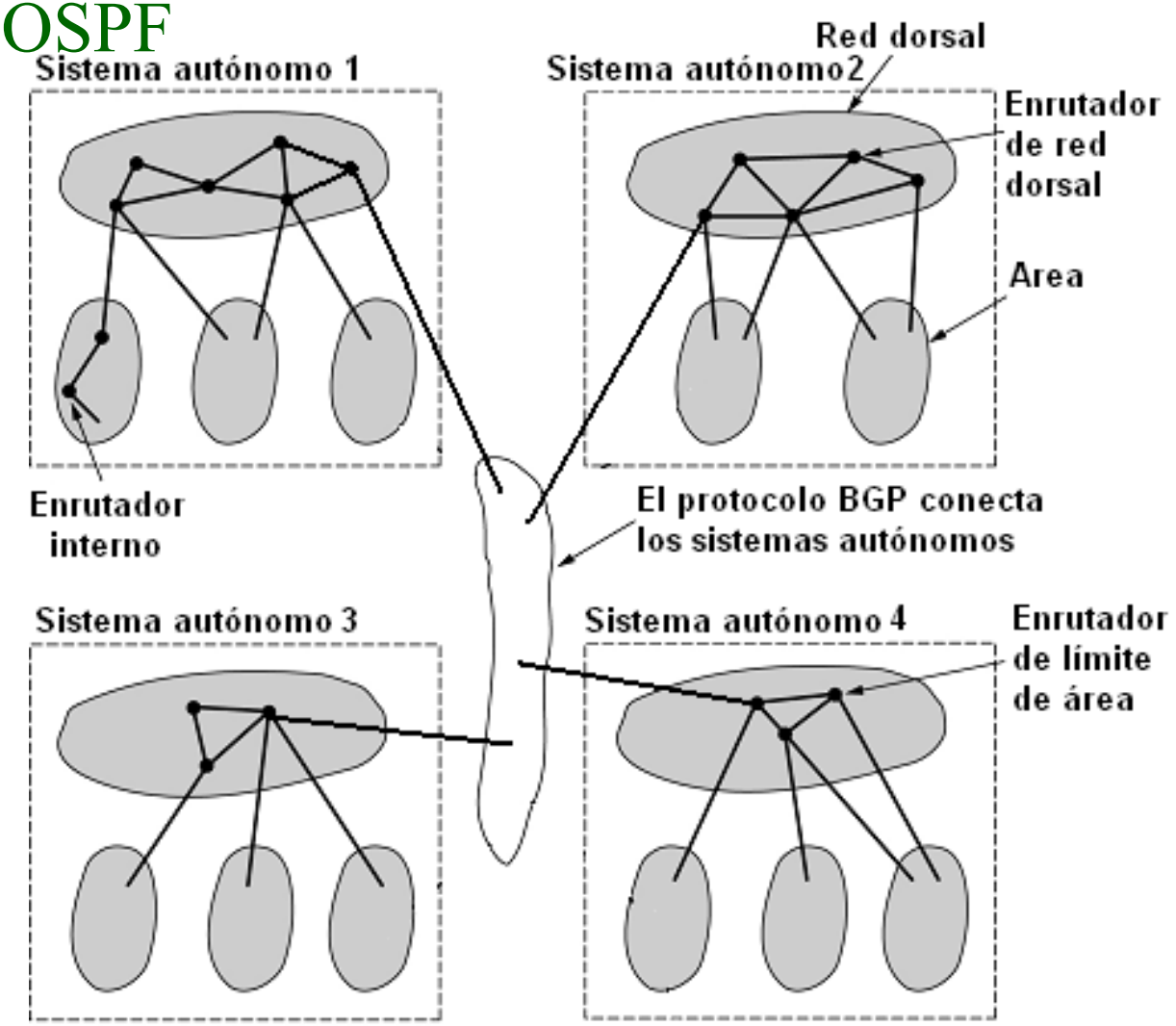
- Los routers OSPF mantienen, además de la tabla de enrutamiento, una base de datos de adyacencia y una base de datos topológica.
- La base de datos de adyacencia es un lista de los vecinos con los cuales se ha establecido una comunicación bidireccional. No todos los vecinos se consideran adyacentes.
- La base de datos topológica contiene una imagen completa y sincronizada de la red.
- El algoritmos de la ruta más corta determina la mejor ruta hacia un destino que es la que menos costo tenga. Generalmente el costo de cada enlace es el ancho de banda.
- La ruta de menor costo se agrega a la tabla de enrutamiento, que se conoce también como la base de datos de envío.
- Para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los routers de OSPF seleccionan un router designado (DR) y un router designado de respaldo (BDR) que sirven como puntos de enfoque para el intercambio de información de enrutamiento.

Terminología OSPF

- Muchos de los sistemas autónomos en Internet son grandes por sí mismos y nada sencillos de administrar, por lo que se dividen en áreas numeradas, donde un área es una red o conjunto de redes inmediatas. Cada sistema autónomo tiene un área de red dorsal, llamada 0. Todas las áreas se conectan a la red dorsal. La topología de la red dorsal no es visible fuera de ésta.

- OSPF distingue cuatro clases de enrutadores:
  1. Enrutadores internos que están totalmente dentro de una área.
  2. Enrutadores de límite de área que conectan dos o más áreas.
  3. Enrutadores de la red dorsal.
  4. Enrutadores fronterizos de sistemas autónomos que se comunican con los enrutadores de otros sistemas autónomos.

Conceptos OSPF



Relación entre sistemas autónomos, redes dorsales y áreas en OSPF

Conceptos OSPF

- OSPF es apropiado para internetworks grandes y escalables y la mejor ruta se determina en base a la velocidad del enlace (el costo). Cuanto mayor sea la velocidad, menor será el costo de OSPF del enlace.
- Después de la convergencia OSPF inicial, el mantenimiento de un estado convergente es más rápido porque se inundan los otros routers del área solamente con los cambios en la red. Sin embargo, la convergencia inicial puede ser lenta.
- OSPF no tiene límites de tamaño. Si la red se divide en áreas, se puede jerarquizar la red y lograr más eficiencia y mejor escalabilidad.
- OSPF requiere routers más poderosos y más memoria que RIP ya que el algoritmo de la ruta más corta (o algoritmo de Dijkstra) es complejo.

CONCEPTOS OSPF

- OSPF soporta tres tipos de conexiones y redes:
  1. Las líneas punto a punto entre dos enrutadores, sólo existen dos nodos y no se elige ningún DR ni BDR. Ambos routers llegan a ser completamente adyacentes entre sí.
  2. Redes de multiacceso con capacidad difusión, tal como Ethernet: no se sabe de antemano cuántos routers estarán conectados. Se elige un router designado (DR) que se hace adyacente a todos los demás routers del segmento de broadcast. Además se elige un segundo router como router designado de respaldo (BDR) para que se haga cargo de las responsabilidades del DR en caso de que éste fallara
  3. Redes de multiacceso sin capacidad de difusión, tal como Frame Relay, X.25 y ATM.
- Una red de multiacceso es la que puede tener múltiples enrutadores, que se pueden comunicar directamente con los demás.
- OSFP funciona resumiendo la colección de redes reales, enrutadores y líneas con un grafo dirigido en el que a cada arco se asigna un costo (distancia, retardo, saltos, etc) entonces calcula la ruta más corta con base en los pesos de los arcos.

FUNCIONAMIENTO OSPF

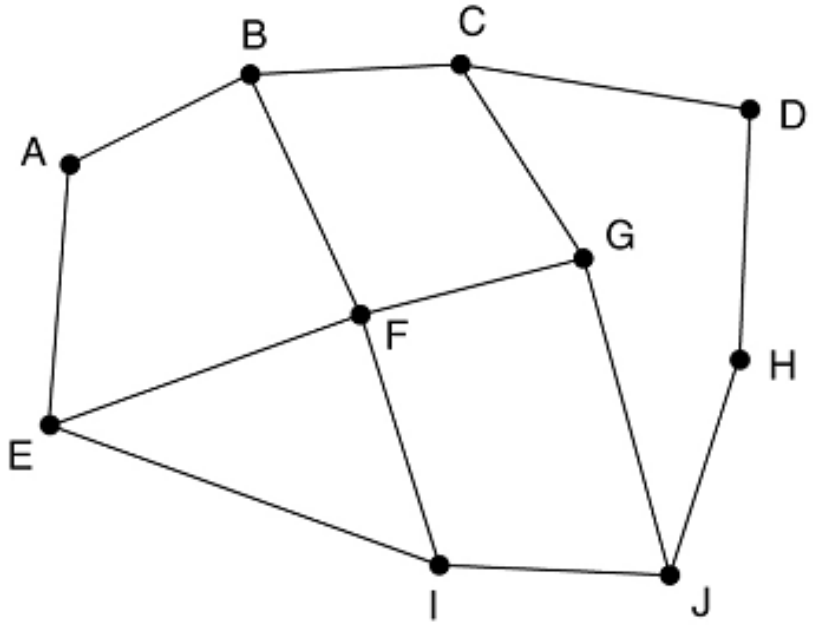
- Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz, envía un paquete Hello. Los routers OSPF utilizan los paquetes Hello para iniciar nuevas adyacencias y asegurarse de que los routers vecinos sigan funcionando. Los Hellos se envía a intervalos regulares.
- En las redes multiacceso, el protocolo Hello elige un router designado (DR) y un router designado de respaldo (BDR). Estos router mantienen adyacencias con todos los demás routers OSPF en la red.
- Los routers adyacentes pasan por una secuencia de estados. Los routers adyacentes deben estar en su estado completo antes de crear tablas de enrutamiento y enrutar el tráfico.
- Cada router envía publicaciones del estado de enlace (LSA) en paquetes de actualización del estado de enlace (LSU). Cada router que recibe una LSA de su vecino registra la LSA en la base de datos del estado de enlace.
- Con la información recibida de los vecinos y costos, cada enrutador construye el grafo para su área y calcula la ruta más corta. Lo mismo ocurre a nivel de área de red dorsal y los enrutadores de límite de área se encargan de difundirlo dentro de su área

Protocolo BGP

- Se utiliza para la comunicación entre sistemas autónomos, y está muy influenciado por la política, seguridad o economía que impone limitaciones al enrutamiento
  Ejemplos:
  1. Ningún tránsito a través de ciertos sistemas autónomos.
  2. Nunca ponga Irak en una ruta que inicie en el Pentágono.
  3. No pasar por Estados Unidos para llegar de México a Panamá.
  4. Transite por Albania sólo si no hay otra alternativa al destino.
  5. El tráfico que empieza o termina en IBM no debe transitar por Microsoft.

Estas políticas se configuran manualmente y no forman parte de BGP

Protocolo BGP



(a)

Información sobre D que F recibe de sus vecinos

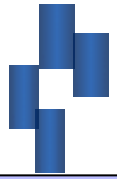
De B: "Yo uso BCD"
De G: "Yo uso GCD"
De I: "Yo uso IFGCD"
De E: "Yo uso EFGCD"

(b)

(a)Conjunto de enrutadores BGP (b) Información enviada a F

Utiliza un protocolo parecido al vector de distancia, llamado **protocolo de vector de ruta**, donde cada enrutador en lugar de mantener el costo para cada vecino, guarda el registro de la ruta utilizada.

En la figura se muestra un ejemplo donde el enrutador F, quiere actualizar su camino a D.



Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

Multidifusión en Internet

- La comunicación normal IP está entre un emisor y un receptor. Sin embargo para algunas aplicaciones es útil que un proceso pueda enviar simultáneamente a una gran cantidad de receptores.
- IP apoya la multidifusión, usando direcciones de clase D.
- Cada dirección de clase D identifica un grupo de host. Hay 28 bits disponibles para identificar los grupo, de modo que pueden existir al mismo tiempo más de 250 millones de grupos.
- Se soportan dos tipos de direcciones de grupo: las permanentes y las temporales.
- Ejemplos de direcciones de grupo permanentes:
  - 224.0.0.1 Todos los sistemas en una LAN.
  - 224.0.0.2 Todos los enrutadores en una LAN.
  - 224.0.0.5 Todos los enrutadores OSPF en una LAN.

Multidifusión en Internet

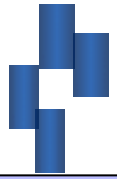
- Los grupos temporales se deben crear antes de que se puedan usar. Un proceso puede pedir a su host que se una a un grupo específico. También puede pedirle que deje el grupo.
- Cada host conserva el registro de a qué grupos pertenecen actualmente sus procesos.
- La multidifusión se implementa mediante enrutadores de multidifusión especiales. Alrededor de una vez por minuto, estos enrutadores solicitan a los hosts información de los grupos de sus procesos.
- El protocolo para la gestión de la adscripción dinámica se denomina IGMP (Internet Group Management Protocol).
- El enrutamiento de multidifusión se crea utilizando árboles de difusión
    - Cada enrutador de multidifusión intercambia información son sus vecinos.
    - Cada enrutador contruye un árbol de expansión por grupo que cubra a todos los miembros de dicho grupo.
    - Se emplean varias optimizaciones para recotra el árbol y eliminar los entrutadores y redes que no estén en grupos.

Protocolo de administración de grupos IGMP

- IGMP, Internet Group Management Protocol, RFC 2236.
- Permite gestionar la subscripción o abandono de miembros de un grupo de multidifusión.
- Opera entre el receptor y el primer enrutador que interconecta su red a otras.
- Ofrece tres operaciones básicas:
  - Consulta de pertenencia: el enrutador puede consultar a los sistemas finales directamente conectados al mismo si pertenecen a un grupo de multidifusión, y a qué grupos.
  - Informe de pertenencia: los sistemas finales pueden devolver este tipo de respuesta ante la consulta de pertenencia. También pueden emitir este tipo de informes cuando una aplicación desee unirse a un grupo de multidifusión.
  - Abandono de grupo: esta operación es opcional. Indica la solicitud de un receptor para abandonar un grupo de multidifusión.

Protocolo de administración de grupos IGMP

- Para unirse a un grupo
  - Un host envía un mensaje de informe, en el cual el campo de dirección del grupo es la dirección multidifusión del grupo. Este mensaje se envía en un datagrama IP.
  - Todos los hots que son miembros actuales de este grupo de multidifusión reciben el mensaje y tiene conocimiento del nuevo miembro del grupo.
- Comprobación de continuidad de un grupo
  - Para mantener una lista actual válida de las direcciones de grupos activos.
  - Un dispositivo de encaminamiento de multidifusión emite periódicamente mensaje de petición con dirección de multidifusión *todos–los-hots*.
  - Cada computador que quiera seguir permaneciendo como miembro del grupo debe atender los datagramas contestando con un mensaje de informe para cada grupo al cual reclama su pertenencia.
  - Para optimizar, en el momento que se escucha un mensaje de pertenencia de un host, los demás esperan un tiempo (temporizador) para responder.



Tema 3. La capa de red de Internet

1. Internet
2. El protocolo IP
3. Direcciones IP
4. Protocolos de control en Internet
5. Protocolos de enrutamiento en Internet
6. Multidifusión
7. IPv6

IPv6

- Si bien IPv4 pueden durar unos pocos años más, debido a las modificaciones que se han ido realizando, sabemos que los días de IP en su formato actual, IPv4, tiene los días contados. Al ver estos problemas se comenzó en 1990 a trabajar en una versión nueva de IP cuyas metas principales fueran:

1. Manejar miles de millones de hosts.
2. Reducir el tamaño de las tablas de enrutamiento.
3. Simplificar el protocolo, para procesar más rápido los paquetes.
4. Proporcionar mayor seguridad.
5. Prestar mayor atención al tipo de servicio, especialmente con datos en tiempo real.
6. Permitir que el protocolo evolucione.
7. Permitir que el protocolo viejo y el nuevo coexistan por años.

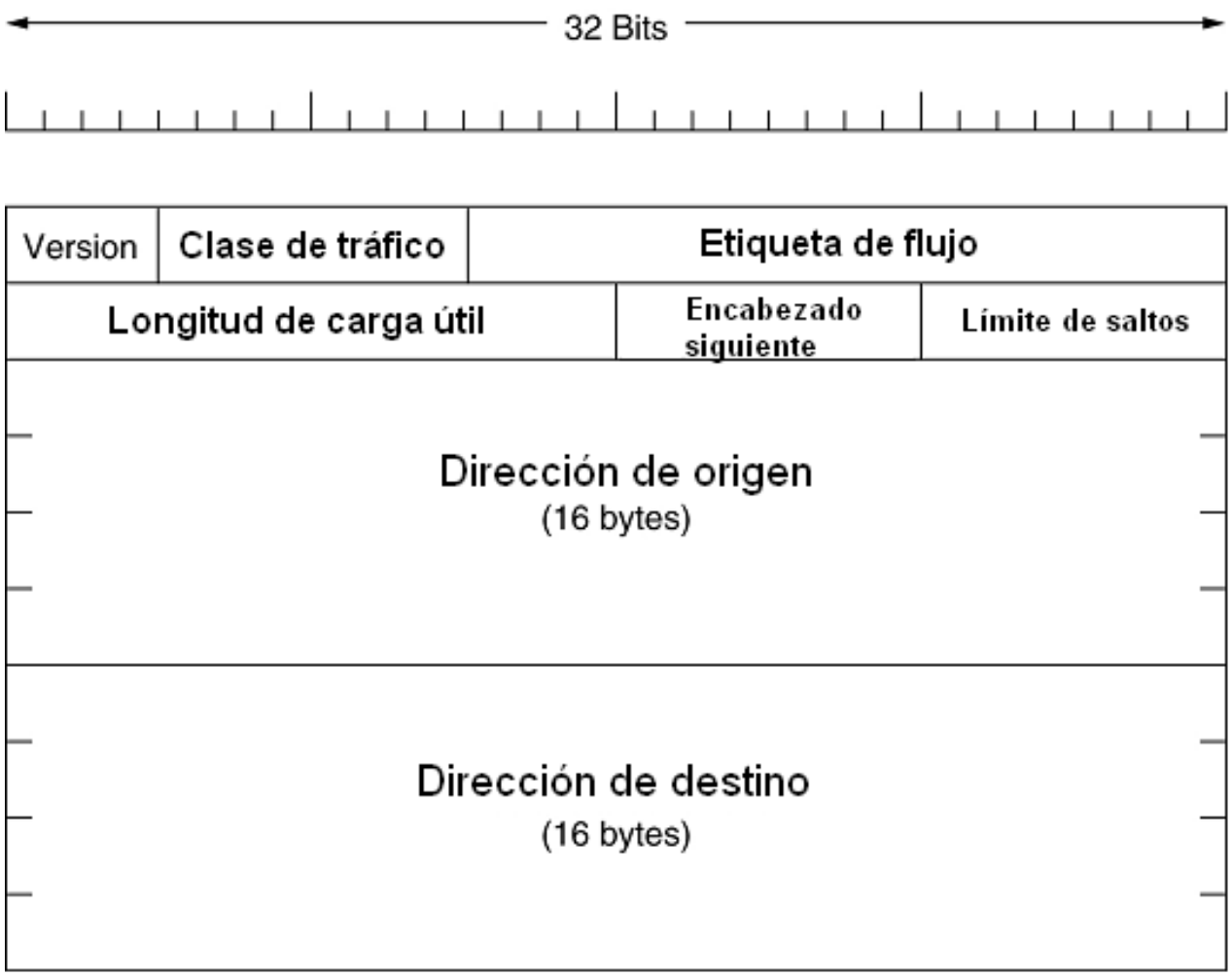
Después de muchas propuestas en 1993 se seleccionaron las mejores y se creó una versión llamada ahora SIPP (Protocolo Simple de Internet Mejorado) y se le dió la designación IPv6.

IPv6

- Características principales de IPv6

1. IPv6 puede representar más direcciones que IPv4 (tiene 16 bytes reservados para ello).
2. Simplificación del encabezado (7 campos frente a los 14 de IPv4).
3. Mejor apoyo de las opciones (campos antes obligatorios son ahora opciones). Mejorar la representación para que sea más fácil omitirlos en el caso de no necesitarse.
4. Mejora en la seguridad. Se incluye autentificación y privacidad.
5. Mayor atención a la calidad del servicio.

IPv6



Encabezado fijo del IPv6

IPv6

- Versión: siempre es 6 para IPv6 y 4 para IPv4.
- Clase de tráfico: se usa para distinguir entre los paquetes con requisitos diferentes de entrega en tiempo real.
- Etiqueta de flujo: aún es experimental, pero se usará para permitir a un origen y a un destino establecer una pseudoconexión con propiedades y requisitos particulares, por ejemplo de retardo, ancho de banda, etc.
- Longitud de carga útil: indica cuántos bytes siguen al encabezado de 40 bytes, ya no hay opciones como en IPv4 pero se agregan los encabezados de extensión.
- Encabezado siguiente: indica cuál de los seis encabezados de extensión de haberlos sigue a este encabezado IP.
- Límite de saltos: se usa para evitar que los paquetes vivan eternamente, igual a TTL de IPv4.
- Dirección de origen y destino de 16 bytes.

IPv6

- Se ha desarrollado una nueva notación para describir direcciones de 16 bytes (IPv4 eran 4): se escriben como ocho grupos de cuatro dígitos hexadecimales, separados los grupos por dos puntos, como sigue:

  8000:0000:0000:0000:0123:4567:89AB:CDEF

Optimizaciones:

Ya que muchas direcciones tendrán muchos ceros en ellas, se pueden optimizar, primero quitando en un grupo los ceros de la izquierda (0123 se puede reemplazar por 123) y reemplazar uno o más grupos de 16 ceros por ::, por lo que quedaría

8000::123:4567:89AB:CDEF

Las IPv4 se pueden representar como ::192.21.20.46

Hay disponibles 2^{128} direcciones disponibles o lo que es lo mismo 3 * $10^{38.}$ Si la Tierra completa incluida los océanos, estuviera cubierta de computadoras, el IPv6 permitiría $7*10^{23}$ direcciones IP por metro cuadrado.

IPv6

- Como ya no es necesario el campo de Opciones de IPv4, se introdujo el concepto de encabezado de extensión (opcional). Estos encabezados pueden usarse para proporcionar información extra, pero codificada de manera eficiente. Hay seis tipos de encabezado que se listan en tabla

Encabezado de extensión	**Descripción**
Opciones salto por salto	Información diversa para enrutadores
Opciones de destino	Información adicional para el destino
Enrutamiento	Ruta total o parcial a seguir
Fragmentación	Manejo de fragmentos de datagramas
Autenticación	Verificación de la entidad del emisor
Carga útil de seguridad encriptada	Información sobre el contenido encriptado

Encabezados de extensión IPv6

Diferencias con IPv4

- Se retiró el campo IHL, porque el encabezado tiene una longitud fija.
- El campo de Protocolo se retiró porque el campo Encabezado siguiente, indica lo que sigue al último encabezado IP (un segmento UDP o TCP).
- Se retiraron todos los campos que tenían que ver con la fragmentación. Ahora es el host y no el enrutador quien debe fragmentar si es necesario los paquetes para que los pueda tratar el enrutador.
- La suma de verificación desaparece, porque su cálculo reduce en gran medida el desempeño, además ya este se realiza en la capa de enlace de datos y la de transporte.
- Por supuesto, se aumentó el tamaño en byte de la dirección de origen y destino.

BIBLIOGRAFÍA

- A. S. Tanenbaum. Redes de Computadoras, 4ª Edición. Prentice-Hall, 2003.
- W. R. Stallings. Comunicaciones y Redes de Computadoras, 7ª Edición. Prentice-Hall, 2004.
- W.R. Stevens. TCP/IP Illustrated, Vol.1 The Protocols, Ed. Addison Wesley, 2000.